**Revista Brasileira de Engenharia Biomédica,**
v. 23, n. 1, p. 53-77, abril 2007

ISSN 1517-3151

**Artigo de Revisão**
Recebido em 19/05/2006 e aceito em 27/02/2007

# Segurança em informações médicas: visão introdutória e panorama atual

*Security in medical information: overview and current scenario*

**Luiz Octávio Massato Kobayashi***
Escola Politécnica da USP
São Paulo, Brasil

Instituto do Coração (InCor) HC-FMUSP
Av. Dr. Enéas de Carvalho Aguiar, 44, 2º andar
CEP: 05403-000, Cerqueira César - São Paulo - SP
e-mail: luiz.kobayashi@incor.usp.br
Tel: (11) 3069-5545

**Sérgio Shiguemi Furuie**
Instituto do Coração (InCor) HC-FMUSP
São Paulo, Brasil

*Autor para correspondência

**Resumo**
Com a disseminação dos sistemas informatizados para a área da saúde, a questão da segurança da informação passa a assumir uma importância cada vez mais crucial, visando principalmente resguardar um dos direitos fundamentais do paciente, qual seja, a privacidade das suas informações, uma vez que a manipulação indiscriminada de informações acerca da saúde da pessoa pode acarretar danos irreparáveis de ordem física e moral. Além disso, o comprometimento da confiabilidade de tais informações pode minar a credibilidade das instituições de saúde e prejudicar a pesquisa, na medida em que dados incorretos levarão naturalmente a diagnósticos e resultados incorretos. Apesar da relevância que a segurança possui, o desenvolvimento de soluções voltadas para a área médica é algo relativamente recente. Isso porque existem várias características específicas para esta área, o que requer uma visão sobre o contexto das informações médicas – em particular, os aspectos éticos e legais – para que se possa atender de forma adequada os seus requisitos e implantar os mecanismos tecnológicos condizentes. Este artigo apresenta um panorama geral da segurança em informações médicas, fazendo primeiramente algumas considerações chave sobre a segurança da informação de um modo geral e o contexto de segurança na área médica, para então mostrar as propostas e implementações realizadas em várias frentes visando garantir os diferentes aspectos da segurança das informações médicas.
**Palavras-chave:** Informática médica, Privacidade, Segurança, Sistema de informações em saúde.

***Abstract***
*The increasing adoption of information systems in healthcare leads to a scenario where information security plays a crucial role in order to protect one of the most fundamental rights of the patient: his/her privacy. Breaches in privacy may lead to irreparable damage, physically, morally and socially to the patient. Moreover, the credibility of the information may be shaken, compromising the reputation of the healthcare institution and affecting medical research in a negative way, for wrong data will naturally result in wrong diagnosis and conclusions. Despite the relevance of security in healthcare information infrastructure, only recently research has been carried out in this field. It must be noticed that there are specific constraints for this field, which requires a deep knowledge on the information context, with emphasis in the ethical and legal aspects. One can, then, adequately elicit and meet the requirements needed and implement the technological mechanisms. This article presents an overview on healthcare information security, starting with some key issues in information security and then presenting the several proposals and implementations done up to now.*
***Keywords****: Healthcare information systems, Healthcare informatics. Security, Privacy,*

## Extended Abstract

***Introduction***

*Health and welfare are among the most fundamental needs of humanity. With the advent of modern information systems, there was a gradual transition from paper records to electronic patient records (EPR) and now, the use of computers in the healthcare field has been widespread.*

*However, this generates a huge amount of information to be acquired, stored, processed and managed, raising concerns about security and privacy of patient data. The lack of adequate controls, procedures and policies may hamper the usage or even render the information systems useless, for the patients and physicians will refuse to provide their personal information, fearing that it may fall on the wrong hands. Therefore, security has been playing an increasingly crucial role in healthcare information systems.*

*This work intends to present the current scenario of healthcare information security, focusing on the application level security services, like integrity, authenticity, confidentiality and accountability.*

***Methods***

*Security is an intuitive concept, but also very vague, given the multitude of aspects that it comprehends. Therefore, one must take into account the context of the problem to develop a satisfactory security solution.*

*There are three essential observations that must be made about security:*

- *Security is not merely a technological issue, depending also on organizational and personnel issues.*
- *There is no such thing as total security. There is a need to balance costs and benefits of security measures in order to develop an adequate infrastructure.*
- *Security is always an evolutive process. An outdated implementation may be useless, or even worse, hinder the usage of the systems.*

*Hence, one must envision first the context where security will be applied, and then elicit the requirements and the risks, to develop top-level architectures and frameworks which will be translated into security services. In the healthcare field, the context presents a complex scenario, with several different users associated with different profiles accessing a vast amount of many kinds of information scattered in several systems, with a legal framework imposing a number of constraints.*

*There are a number of goals that security is intended to meet, like providing privacy of patient data, increase the responsibility of the practitioners and reduce costs by secure digital exchange of information. This can be mapped into requirements like the records being trustworthy and authentic and the data communication and storage being secure. The proposals made so far are aimed at meeting these requirements in different aspects and levels.*

***Results***

*There are several working groups in national and transnational levels, specifically addressing security issues in healthcare. The most famous is probably IMIA (International Medical Informatics Association) and its Working Group 04, but there are other initiatives by ISO and by standards like DICOM and HL7. The European Community has launched several researches on healthcare information security, and countries like Japan, Australia and Malaysia have also promoted the creation of research groups. In Brazil, SBIS (Brazilian Society of Healthcare Informatics) is the one who is most active in this field.*

*There have been several approaches for security policies and high level management, where the HORUS model, proposed by NHS (National Health Service) plays a proeminent role. There are also some proposals for policy development and deployment.*

*As for the security frameworks and architectures, there is a tendency to use a view based on components, with an increasing popularity of architectures like MDA (Model Driven Architecture) and SOA (Service Oriented Architecture).*

*The communication security has already been addressed in several works. The fundamentals have been laid on secure tunneling and TTP (Trusted Third Parties) for authentication. The most recent works explore additional features, like user interfaces, access tracking and security policy translations. Moreover, the advent of pervasive computing asks for security in mobility.*

*The application security, on the other hand, can be spawned into different security services. For integrity and authenticity, the most popular approaches are digital signatures and watermarking, though there is some resistance in using watermarking. For confidentiality, identification and accountability, there are only few works to protect data, as opposed to access control, where a number of works has been done in order to prevent unauthorized access to sensitive patient information. Likewise, there are several works on privacy, which can be seen as a combination of the aforementioned security services.*

***Discussion***

*The works on healthcare information security can be divided into two kinds: a wider approach, usually supported by governmental initiatives, where a reference implementation, architecture or methodology is proposed and/or validated; and a narrower approach, taken by academic research, aiming at a specific security issue. There are still a number of challenges to be addressed, like long term storage, end-to-end security and anonymization, offering several opportunities for researchers, especially in Brazil, where there are almost no academic efforts in this field.*

## Introdução

A saúde é uma das necessidades mais fundamentais da sociedade e, portanto, está intimamente presente na sociedade moderna, como atesta o Artigo XXV da Declaração Universal dos Direitos Humanos (Organização das Nações Unidas, 2004), que contempla o direito do ser humano de ter acesso à saúde e aos cuidados médicos.

Com a introdução das modernas tecnologias de informação e comunicação no campo médico, houve a gradual evolução de prontuários em papel para Registros Eletrônicos de Saúde (RES) do paciente. Shortliffe (1998) aponta para a crescente percepção das ineficiências e frustrações associadas ao uso de registros médicos baseados em papel, especialmente quando o acesso inadequado a informações clínicas é uma das principais barreiras que os clínicos encontram quando tentam aumentar sua eficiência para atender a metas de produtividade.

A tecnologia de informação permeia hoje todas as atividades de um hospital. Mesmo em um centro de tamanho médio, os visitantes entram em contato com o sistema de admissão, que rastreia não somente a admissão de pacientes e dos tratamentos dispensados, mas também monitora a disponibilidade de leitos e infra-estrutura de suporte. Em determinados setores, existe um conjunto de terminais para a equipe de enfermagem para a monitoração de sinais vitais, usando dados coletados por equipamentos presentes em cada quarto. Os farmacêuticos prescrevem medicamentos, verificam interações de drogas e mantêm um controle de inventário usando sistemas *online* para farmácia.

Em alguns centros, médicos utilizam-se da telemedicina para diagnosticar e tratar pacientes em locais remotos. Entre os centros, os registros de saúde e o sistema de cobrança rastreiam a evolução do paciente e provêem os dados necessários para seguradoras de saúde. Dwivedi *et al*. (2003) apontam até mesmo para uma disseminação transnacional dos registros médicos do paciente através do acesso Web.

Entretanto, essa grande quantidade de informações a ser adquirida, armazenada, processada e gerenciada levanta uma questão bastante delicada, a da segurança e da privacidade dos dados do paciente, que remonta à antigüidade com o juramento de Hipócrates (Juramento de Hipócrates, 2004). Raghupathi e Tan (2002) lembram que o prospecto de armazenar informações de saúde na forma eletrônica suscita discussões acerca de padrões, ética, privacidade, confidencialidade e segurança.

A falta de controles apropriados, procedimentos e políticas pode levar tais sistemas a estimularem usuários não autorizados a acessar e até mesmo utilizar de forma inadequada as informações associadas com usuários legítimos. Se tais preocupações não forem discutidas, a indústria da saúde pode ser desencorajada a usar as ferramentas de tecnologia da informação e os consumidores de saúde (pacientes, corpo clínico, etc.) irão hesitar em compartilhar as suas informações pessoais, comprometendo a qualidade do tratamento, bem como a pesquisa médica em si.

Desta forma, a segurança assume um lugar de destaque cada vez maior na área de saúde, para garantir que as informações sejam precisas, oriundas de fontes confiáveis e acessadas apenas pelas pessoas corretas.

Este trabalho tem por objetivo apresentar o panorama atual da segurança em termos tecnológicos para a área de informações médicas, partindo-se de uma visão geral sobre segurança como um todo, para então estreitar o escopo nos avanços tecnológicos obtidos para a área.

## Escopo

O número de aspectos associados à segurança em aplicações médicas é muito vasto. Para fins deste artigo, decidiu-se limitar o escopo a aspectos em nível de aplicação, tais como integridade, auditabilidade, confidencialidade, autenticidade e controle de acesso. Alguns aspectos muito relevantes não são discutidos aqui, mas a intenção não é diminuir a sua importância. Por exemplo, não são discutidos: tolerância a falhas, mecanismos de recuperação, sistemas operacionais seguros, métodos gerenciais para definição, estabelecimento e implantação de políticas e procedimentos de segurança, resistência em utilizar ou confiar em sistemas computadorizados, geração de senhas, treinamento, facilidade de uso, manutenção e administração de sistemas, vírus e similares (*trojans*, etc.), *backups* seguros, segurança de *hardware*, segurança física, erros humanos de entrada de dados e garantia de qualidade.

**Considerações gerais sobre segurança** – A segurança é um conceito intuitivo, mas ao mesmo tempo extremamente vago por causa da vastidão de aspectos que ela compreende. Neumann (2005) cita alguns casos reais de riscos em termos de segurança na área médica em diferentes aspectos, incluindo aspectos físicos, que prejudicaram em maior ou menor grau o atendimento aos pacientes. Uma análise em termos de segurança deve ser bastante ampla, levando-se em consideração o contexto no qual a segurança é mencionada.

Para que tal análise seja apropriada, primeiramente devem-se ressaltar três pontos essenciais sobre a

segurança:

1) ***A segurança não é uma questão meramente tecnológica***. As ferramentas tecnológicas são apenas instrumentos que podem, ou não, ser aplicados de forma eficaz. São necessários meios para definição e adoção de boas práticas, bem como meios para detectar e punir eventuais transgressões. Isso implica em abordar a segurança em âmbito organizacional, com a definição, implantação e manutenção de políticas, procedimentos e mecanismos, e em âmbito pessoal, com treinamentos e ética. Em última análise, pode-se dizer que a segurança é um problema em termos de pessoas, não em termos de tecnologias (Niinimäki *et al*., 1998).
2) ***Não existe segurança total***. Por melhor que seja a segurança implantada, sempre é possível burlá-la, tendo-se os recursos necessários e suficientes. A máxima "não existe corrente mais forte do que o seu elo mais frágil" se aplica de forma perfeita à segurança. Apenas a título de exemplo, por melhor que sejam as políticas, procedimentos, mecanismos e treinamentos, um usuário legítimo, mas desonesto, pode perfeitamente tomar posse de informações que não lhe pertencem. É bom lembrar que o nível de segurança atingido depende do nível de confiança que se assume acerca das medidas nos níveis organizacional, pessoal e tecnológico (Pfitzmann e Pfitzmann, 1992).
3) ***A segurança é um processo evolutivo e não um projeto rígido e fechado***. É ingenuidade acreditar que a implantação da segurança terá um término bem definido. As mudanças nas regras de negócio e as evoluções tecnológicas pedem por um acompanhamento e uma atualização contínuos dos projetos de segurança, para evitar que esta se torne inócua ou, ainda pior, um fardo que impede que as tarefas sejam executadas a contento.

Em termos tecnológicos, a menção à segurança traz à mente conceitos como criptografia, controle de acesso e integridade dos dados. Entretanto, cabe lembrar a necessidade da existência de uma infra-estrutura tecnológica, que compreenda não apenas os mecanismos, mas também uma arquitetura que forneça o contexto em que eles serão utilizados, e as diretrizes de planejamento que irão definir tal arquitetura. As exigências legais também devem ser devidamente contempladas durante o planejamento.

A partir disso, deve-se proceder à análise de risco, na qual devem ser levantados os riscos, vulnerabilidades e ameaças que irão determinar os detalhes mais precisos da implementação para melhorar a segurança e a privacidade das informações (Gritzalis *et al*., 2005). Existem vários métodos para se proceder à análise de riscos e implementação, como a proposta por Baur *et al.* (1997). Uma outra abordagem é através da aplicação da norma da ISO 17799, um padrão para gerenciamento de segurança da informação, para a área de sistemas de informação de saúde (Cavalli *et al*., 2004).

Durante essa análise, deve-se ter em mente que os projetos relativos à segurança, incluindo-se os na área médica, trazem consigo o chamado *Princípio da Proporcionalidade*, que estabelece a necessidade de se ter um equilíbrio entre a *utilidade* da aplicação, sistema, ferramenta ou processo a se tornar seguro, e a *segurança e privacidade* das entidades envolvidas. Em outras palavras, deve-se introduzir a segurança de forma que o ônus das suas medidas não seja tão grande a ponto de tornar o sistema impraticável de ser usado (Iachello e Abowd, 2005).

Finalmente, os requisitos levantados pela análise de risco podem ser traduzidos em *serviços de segurança*, tais como confidencialidade, integridade e disponibilidade, que por sua vez podem ser implantados de diversas formas. Existe uma gama bastante grande de serviços de segurança que podem ser introduzidos (Blobel e Roger-France, 2001), como mostra a Figura 1.

**Visão geral sobre o contexto das informações na área da saúde** – Para a implantação de medidas de segurança da informação na área da saúde, é necessário conhecer o seu contexto.

O objetivo dos sistemas de informação em saúde é basicamente prover subsídios para tratamento médico de alta qualidade a todos, a um custo adequado e protegendo os direitos humanos do paciente. A implantação de tais sistemas traz consigo a aquisição, armazenamento e processamento de um volume cada vez maior de informações, que podem ser relacionados entre si para propósitos médicos, econômicos e legais (Biskup e Bleumer, 1996). Com isso, é possível ter diagnósticos mais precisos, aumentando a competitividade da instituição e provendo embasamento legal contra eventuais processos jurídicos.

Cabe lembrar que as informações do paciente podem ser utilizadas por um número muito grande de pessoas das mais variadas instituições (Rindfleisch, 1997), como mostrado na Figura 2.

Para que o tratamento seja de alta qualidade, é necessário entre outras coisas, o acesso à informação certa no tempo certo, na quantidade certa e no local certo e a existência de ferramentas de suporte à decisão. Para tanto, existem alguns grandes desafios a serem

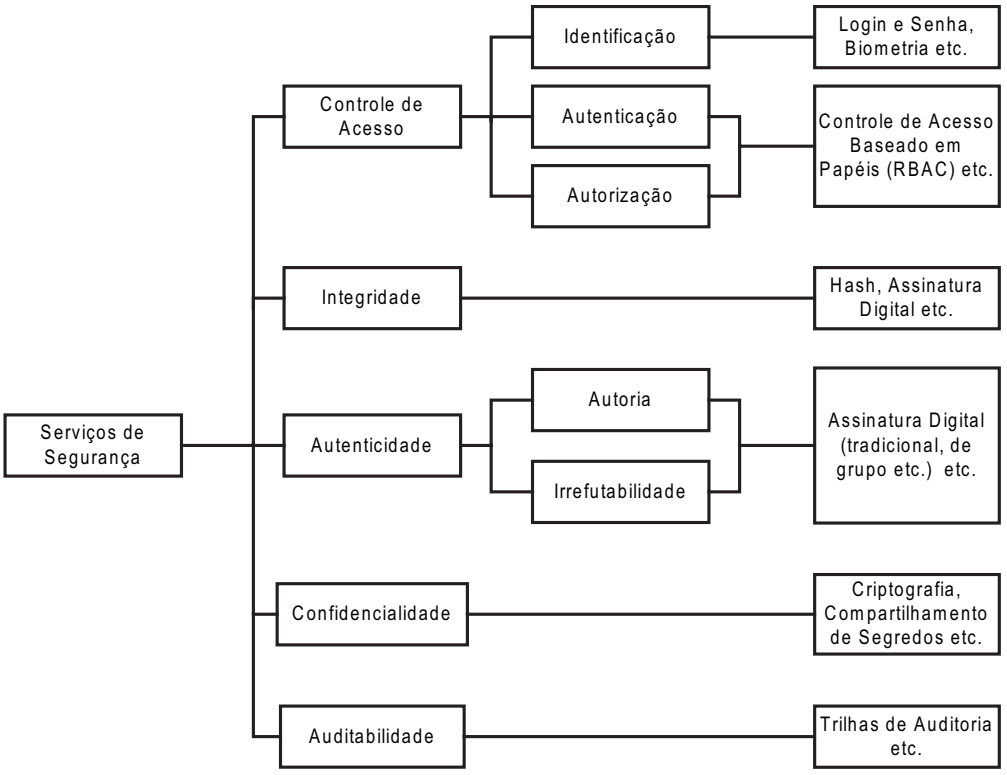


**Figura 1.** Alguns Serviços de Segurança (Blobel e Roger-France, 2001). ***Figure 1.*** *Examples of Security Services (Blobel and Roger-France, 2001).*

resolvidos, incluindo-se a proteção da privacidade, confidencialidade e segurança dos dados (Shortliffe, 1999). Ao mesmo tempo, a introdução do prontuário eletrônico do paciente (PEP), uma entidade que aglutina diversas funcionalidades, centradas no atendimento direto ao paciente (Kwak, 2005), traz à tona uma arquitetura em que diferentes entidades se comunicam entre si, transmitindo e recebendo diversos tipos de dados através da rede interna (Figura 3).

Assim, em conjugação com outros repositórios de dados ligados em rede, uma instituição de saúde pode obter substratos não apenas em termos clínicos, mas também educacionais, administrativos e financeiros. Mais do que isso, é possível utilizar ferramentas de gerenciamento do conhecimento (*knowledge management*), que vêm ganhando importância e destaque crescentes, tanto para a explicitação do conhecimento na área da saúde quanto para a sua disseminação, para a atualização do conhecimento existente e a criação de novos conhecimentos na área clínica e na área da saúde como um todo, permitindo melhor apoio tecnológico para a tomada de decisão (Bali *et al*., 2005). Ou seja, a infra-estrutura de informação em um ambiente institucional apresenta um cenário intrincado, com informações extremamente variadas e de diversos graus de complexidade, onde pessoas e entidades de diversas áreas de atuação acessam tais informações com propósitos bastante distintos em vários tipos de equipamentos – não apenas terminais de computador ou estações de trabalho, mas também equipamentos médicos – e em sistemas também diferentes, que não necessariamente se comunicam entre si.

Ao mesmo tempo, deve-se ter em mente que tal integração pode ser pensada também em nível interinstitucional, visando prover serviços como (Ruotsalainen, 2004):

- Compartilhamento de registros de paciente entre diferentes clínicos;
- Acesso ao prontuário do paciente a qualquer hora em qualquer lugar;
- Consulta, monitoramento e assistência remotos através de conexão à rede;
- Pesquisas relativas a populações de pacientes, visando, por exemplo, a manutenção da saúde pública.

Assim sendo, é possível imaginar uma rede externa (Internet) interconectando várias entidades e instituições, que acessam, compartilham e manipulam

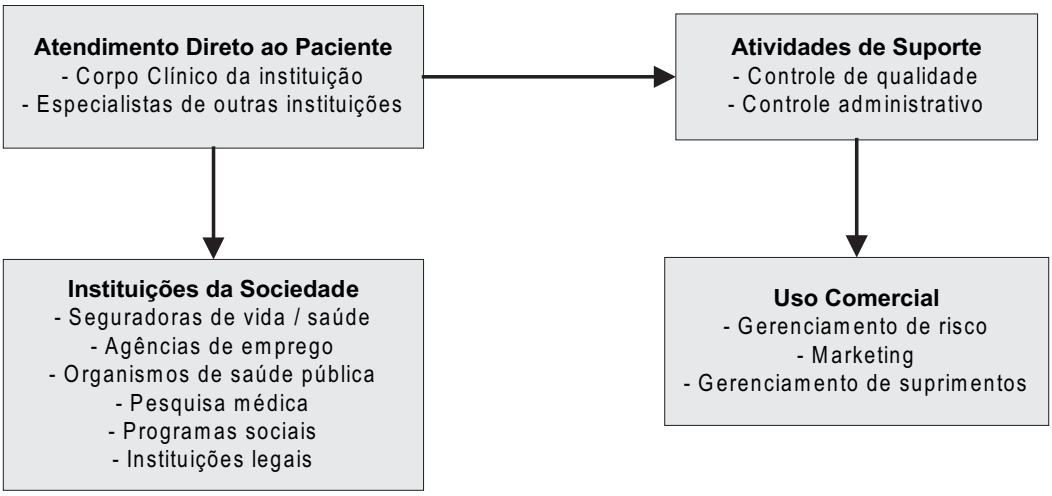


**Figura 2.** Exemplo de algumas entidades que acessam as informações do paciente. As flechas mostram o fluxo de informação. ***Figure 2.*** *Some entities that may access patient information. The arrows show the information flow.*

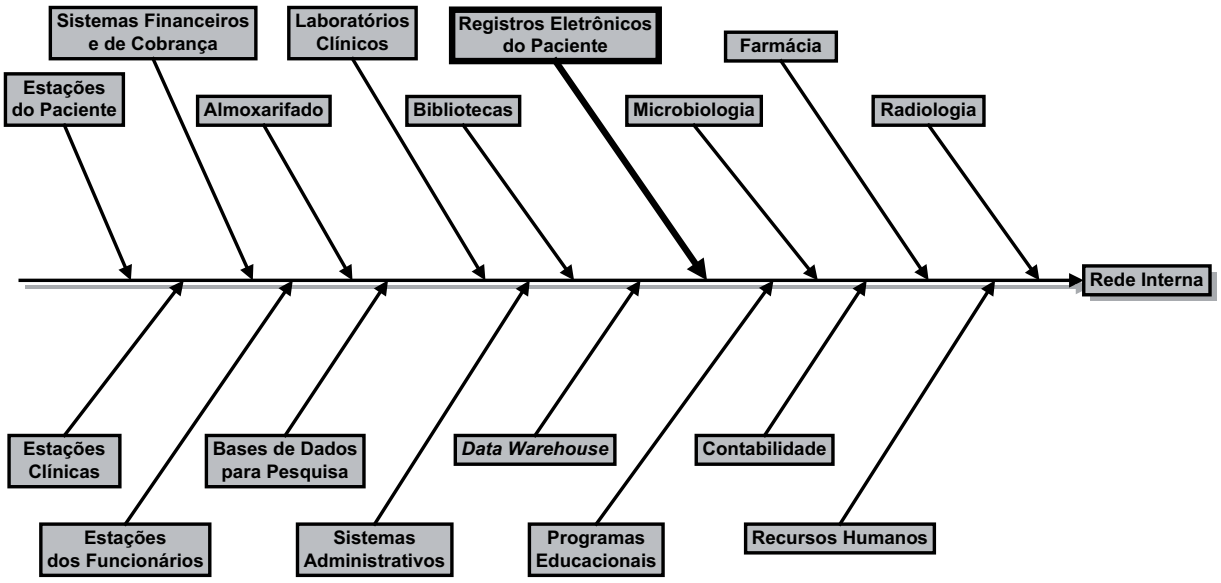


**Figura 3.** Exemplo de uma rede interna de uma instituição de saúde. ***Figure 3.*** *Sample of a healthcare institution's intranet.*

diversas informações da área da saúde com diferentes objetivos para desempenhar as suas tarefas, como ilustra a Figura 4.

Com isso, a complexidade do cenário aumenta ainda mais, uma vez que agora podem existir diferentes sistemas, executando tarefas semelhantes e que não são necessariamente compatíveis. Além disso, a existência de diferentes estruturas organizacionais leva à adoção de políticas que nem sempre podem ser mapeadas facilmente entre as diferentes instituições.

A implantação de medidas de segurança deve levar em conta este panorama complexo, devendo ser robusta e flexível o suficiente para se adequar aos aspectos ético-legais na área da saúde e aos inúmeros tipos de informação e usuários existentes. Deve prover, caso necessário, soluções específicas para atender a determinados aspectos pertinentes a algum tipo de dado, como por exemplo, a questão da integridade e autenticidade das imagens médicas, tendo como meta primária a manutenção da segurança e da privacidade dos dados do paciente, sem prejudicar o atendimento e a pesquisa.

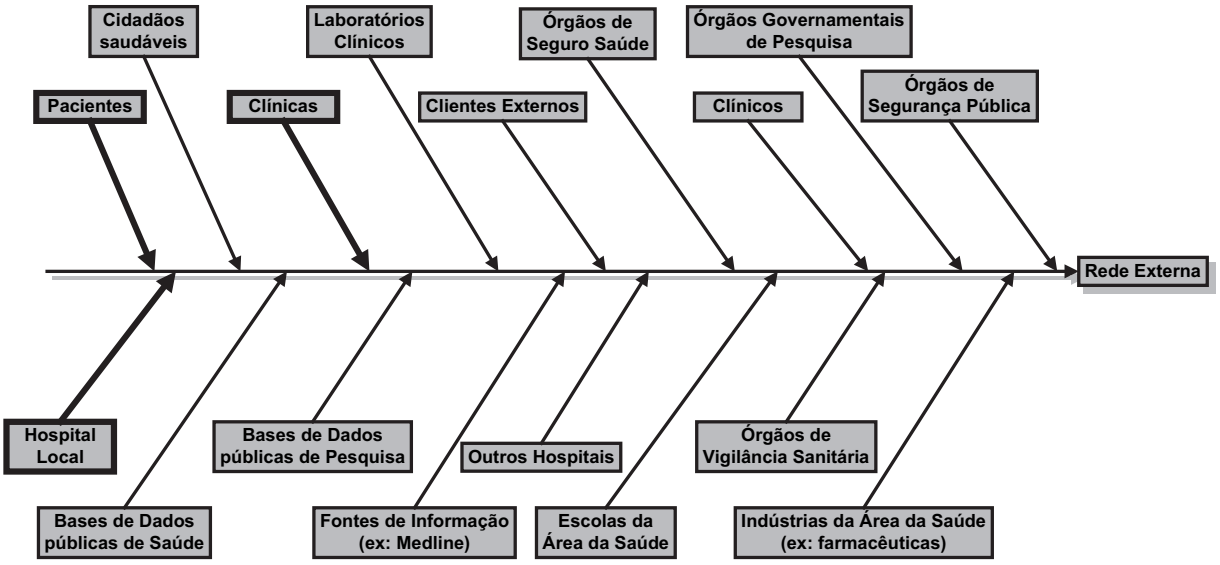


**Figura 4.** Exemplo de rede externa com vários tipos de instituições ligadas. ***Figure 4.*** *Sample view of the internet, showing several types of institutions connected to it.*

**A evolução da conscientização acerca da segurança em informações em saúde** – A segurança é vital para prover duas qualidades fundamentais em informações em saúde: a *confiança* e a *privacidade*. Sem isso, haverá conseqüências sérias (Rindfleisch, 1997). Os pacientes podem evitar a utilização dos serviços de saúde e os clínicos podem se abster de preencher todas as informações acerca do paciente, ou até mesmo manter um registro duplo sobre um mesmo paciente. Além disso, a existência de informações incompletas ou ainda incorretas se reflete de forma profundamente negativa na pesquisa médica, uma vez que dados incorretos levam naturalmente a resultados incorretos (Cushman, 1996).

Note-se que existe um paradoxo inerente aos registros clínicos, que a segurança deve atender: devem-se proteger totalmente os dados do paciente, dada a sua natureza extremamente sensível, ao mesmo tempo em que se deve disseminá-los ao máximo para prover e desenvolver diagnósticos, tratamentos e pesquisas consistentes (Smith e Eloff, 1999).

Em termos digitais, a meta dos sistemas de saúde é prover serviços com alta qualidade para todos, com um custo adequado e de acordo com os direitos humanos do paciente (Biskup e Bleumer, 1996). A tecnologia de informação é uma ferramenta poderosa para se atingir tal meta, mas traz consigo riscos em termos de confidencialidade, anonimato, integridade, acesso a informações e disponibilidade.

Apesar da relevância da segurança da informação para a área da saúde, o seu estudo mais aprofundado tem um início relativamente recente. Embora já em 1974 existisse a preocupação com a segurança na área médica (Dinklo, 1974), foi no início da década de 90 que começaram a surgir com maior freqüência trabalhos sobre o tema, ressaltando-se a importância de aspectos como confidencialidade, atributabilidade e permanência (Rector *et al*., 1991). O reconhecimento da integridade e autenticidade como serviços-chave para as informações médicas, bem como a relevância de se contemplar os aspectos éticos e legais, foram levantados por Essin e Lincoln (1994). Isso foi endossado com o estabelecimento em 1995, nos EUA, de cinco princípios para a guarda das informações do paciente, incluindo a proteção dos dados, limitação e controle do acesso, a auditabilidade e a imputabilidade (May, 1998).

A introdução do Registro Eletrônico do Paciente, em resposta às demandas de melhoria do atendimento (Rindfleisch, 1997), mudou de forma significativa o panorama digital das informações em saúde, reduzindo os custos e definindo o conceito de *shared care*, ou seja, um esforço coordenado de diversos especialistas para prover o melhor diagnóstico, tratamento e acompanhamento do paciente. Contudo, é de suma importância que as informações adquiridas sejam armazenadas de forma consistente em um ambiente distribuído com mecanismos de controle de acesso, para evitar a disseminação indevida de informações sensíveis acerca do paciente, ao mesmo tempo em que elas devem estar

disponíveis o mais rápido possível em situações críticas como emergências (Smith e Eloff, 1999).

Paralelamente, com a maior conscientização da população acerca da informatização dos serviços de saúde, a questão da segurança ganha um foco cada vez maior, necessitando de um planejamento de segurança em nível gerencial dentro da organização, com a definição de estratégias em alto nível, incluindo-se a educação das pessoas envolvidas (Huston, 2001), para garantir a segurança e privacidade dos dados (Petruccio, 2000) dentro de uma relação adequada de custo/benefício. Cabe lembrar que a estimativa dessa relação traz consigo a dificuldade da quantificação do custo associado a erros no tratamento e a necessidade de se contemplar os aspectos específicos à área da saúde, tais como a culpabilidade do clínico ou da instituição, situações de emergência, etc.

A segurança ganha uma importância ainda mais forte com a introdução de dispositivos móveis, com o conceito de *pervasive computing* ou computação ubíqua (Stanford, 2002). A expansão da informatização aumenta naturalmente as vulnerabilidades dos sistemas existentes, já que há um aumento no número de nós que podem ser comprometidos.

Ao mesmo tempo, existe uma quantidade expressiva de equipamentos médicos dentro de um hospital e um número cada vez maior deles contém informações sensíveis do paciente, o que representa uma área substancial de risco para a segurança (Grimes, 2004). Embora tais equipamentos representem uma parcela significativa em termos de geradores de informação em saúde, freqüentemente são ignorados dentro de uma abordagem baseada exclusivamente em segurança para sistemas de informação convencionais. Assim sendo, deve-se considerar, na implantação de medidas de segurança, esses equipamentos biomédicos para que essas medidas sejam mais eficazes. Cabe ressaltar, ainda, os seguintes desafios:

- A diversidade de equipamentos e sistemas médicos que podem coexistir dentro de uma instituição;
- A diversidade de informações que podem ser mantidas e trafegadas na rede, incluindo imagens e sinais fisiológicos;
- O grau de desatualização dos equipamentos médicos em termos de *software* e *hardware*, já que freqüentemente os equipamentos são antigos e há resistência em atualizá-los porque eles funcionam de uma forma estável e os usuários já sabem operá-los;
- A falta de conhecimento interdisciplinar, uma vez que os especialistas na área médica possuem pouco ou nenhum conhecimento sobre segurança da informação e a maioria dos especialistas de segurança de informação, que estão gradativamente assumindo as tarefas de segurança, conhece pouco sobre as tecnologias na área médica (Lorence e Churchill, 2005).

**Aspectos ético-legais da segurança em informações médicas** – As características ético-legais da prática médica são de suma importância dentro da área de segurança em saúde, incluindo-se os sistemas digitais de saúde (McFarland, 1991), pois possuem peculiaridades próprias da área, recebendo uma ênfase bastante pronunciada pelos profissionais da saúde.

O segredo médico é bastante antigo e vem desde o Juramento de Hipócrates, datado do século V A.C., que diz claramente: "àquilo que no exercício ou fora do exercício da profissão e no convívio da sociedade, eu tiver visto ou ouvido, que não seja preciso divulgar, eu conservarei inteiramente secreto" (Juramento de Hipócrates, 2004).

A Associação Médica Mundial adotou várias declarações no tocante ao segredo médico, a começar pela Declaração de Lisboa (Associação Médica Mundial, 2004), que define os direitos do paciente, incluindo o direito à confidencialidade sobre qualquer informação sobre o estado de saúde do paciente, explicitando a necessidade de proteção de todos os dados identificáveis do paciente de acordo com seu arquivamento apropriado. Mas os primeiros esforços nesse sentido surgem já em 1973, com a Declaração de Munique (Associação Médica Mundial, 2004a), que versa sobre o uso de computador na medicina, propondo esforços conjuntos para assegurar a privacidade, a segurança e a confidencialidade de informação dos seus pacientes. Esta declaração foi posteriormente complementada pela Declaração de Tel Aviv (Associação Médica Mundial, 2004b), que definiu a posição da comunidade médica internacional com relação à telemedicina, estabelecendo que as regras do consentimento esclarecido e da confidencialidade do paciente também devem ser aplicadas para o exercício da medicina à distância.

Ao mesmo tempo, em 1999 o Conselho da Europa aprovou a Convenção para a Proteção dos Direitos do Homem e da Dignidade do Ser Humano face às Aplicações da Biologia e da Medicina (Conselho da Europa, 2004), cujo capítulo III, artigo 10, estabelece claramente o direito à privacidade de qualquer pessoa sobre as informações sobre sua saúde, enquanto que, nos Estados Unidos, foi aprovado em 1996 o *Health Insurance Portability and Accountability Act* (HIPAA), que estabelece uma série de diretrizes para o âmbito da saúde em todas as suas formas (Jepsen, 2003), in-

cluindo-se a parte de integridade e autenticidade das informações e normas para uso, acesso e liberação de informações sensíveis (Swire e Steinfeld, 2002).

No âmbito nacional, o segredo das informações do paciente é um direito assegurado pelo artigo 5, inciso X, da Constituição Federal de 1988 (Brasil, 2001), que garante a inviolabilidade da intimidade, da vida privada, da imagem e da honra das pessoas. Diretrizes mais específicas foram estabelecidas pela Portaria do Ministério da Saúde nº 1.286 de 1993 (Brasil, 1994), definindo mais claramente o direito do paciente acerca da manutenção dos seus segredos. Mais recentemente, foi proposto também o Projeto de Lei PL-20/2003 (Brasil, 2003) que versa sobre o mesmo assunto, com uma menção explícita ao prontuário eletrônico, que pode ser considerado como instrumento de evidência legal de acordo com o artigo 225 do novo Código Civil (Brasil, 2001b).

Dentro da comunidade médica nacional, o Conselho Regional de Medicina do Estado de São Paulo publicou em 2001 (Conselho Regional de Medicina do Estado de São Paulo, 2001) a Resolução CREMESP nº 97, tratando sobre a privacidade na rede. E o Conselho Federal de Medicina baixou em 2002 (Conselho Federal de Medicina, 2002) a Resolução CFM nº 1.639/2002, que estabelece normas técnicas para o uso de sistemas informatizados para a guarda e manuseio do prontuário médico, incluindo-se aí a necessidade de manter a integridade da informação e da autenticação.

Em termos de ética, o Código de Ética Médica (Conselho Federal de Medicina, 1988) afirma no Art. 11 sobre o sigilo do médico quanto às informações confidenciais de que tiver conhecimento no desempenho de suas funções, estabelecendo outras diretrizes sobre o mesmo tema também no Capítulo IX. Paralelamente ao Código de Ética Médica, a *International Medical Informatics Association* (IMIA) definiu um Código de Ética para Profissionais de Informática em Saúde que engloba dois princípios, sobre privacidade e sobre segurança, nos quais há diretrizes para que os profissionais de informática em saúde assegurem que os registros eletrônicos, incluindo imagens médicas, sejam armazenados, acessados, utilizados, manipulados ou transmitidos somente para fins legítimos e assegurem a existência de protocolos e mecanismos para monitorar a manipulação de dados contidos nos prontuários, incluindo-se um controle rigoroso sobre a integridade e a autenticidade dos dados (IMIA, 2004).

Em termos jurídicos, cabe ressaltar que existem ainda muitos outros aspectos que devem ser considerados dentro do contexto da saúde, tais como a questão do consentimento esclarecido (Kluge, 2004) e a responsabilidade civil relativa a instituições e profissionais da área de saúde, como é discutido por Cintra (2004), Moreira Filho (2002) e Souza (2002a, 2002b).

**Objetivos e requisitos da segurança das informações em saúde**

Os registros médicos devem ser precisos, acessíveis, autenticados, organizados, confidenciais, seguros, atuais, legíveis e completos (Hamilton, 1992). Ting (1999) ressalta a questão da confiança entre o corpo clínico e o paciente, o que envolve manter de uma forma segura os seus registros. Isso permite obter qualidade da informação, que faz parte do conceito de *information assurance*, um dos principais objetivos da segurança (Voas, 1999), especialmente em sistemas críticos como é o caso dos sistemas de informação para a saúde (Knight, 2002).

Em particular, a introdução da segurança em informações clínicas tem por objetivos:

- Prover a privacidade dos dados do paciente e dos profissionais de saúde através de mecanismos de criptografia e controle de acesso;
- Aumentar a responsabilidade dos empregados na área de saúde e do pessoal administrativo através da auditoria de suas ações e atividades;
- Reduzir custos no setor de saúde através do acesso interinstitucional a dados digitais de uma forma rápida e segura;
- Prover suporte à alta disponibilidade de informação através do uso de grandes redes e conexões de alta velocidade;
- Oferecer um ambiente que permita estabelecer medicina multimídia, telediagnóstico, cirurgias utilizando robôs e telessaúde de maneira confiável.

Para atingir esses objetivos da melhor forma possível, alguns dos principais requisitos de segurança são:

- Os registros devem ter valor legal em caso de serem incluídos em um processo na justiça. Ou seja, os registros devem ser atuais e conter o nome e o momento em que alterações e adições foram feitas nos registros.
- Informações precisas e autenticadas: os registros devem ser íntegros e confiáveis. Um erro, intencional ou não, pode evitar que uma pessoa tenha a informação correta em uma situação crítica. Além disso, é necessário conhecer a procedência da informação para que se possa apurar a responsabilidade por ela.
- Confidencialidade e acessibilidade: as informações relativas à saúde muitas vezes não podem ser re-

veladas (e.g., resultados de teste de HIV, registros de uso de drogas e álcool, registros psiquiátricos). Por outro lado, a questão da acessibilidade é muito importante para os que precisam da informação. Entretanto, nem sempre é possível prever quando e quem terá o direito de acessar as informações – o caso da emergência é um ótimo exemplo. Neste caso, os profissionais de saúde têm a necessidade de se inteirar dos dados do paciente, mas este nem sempre está consciente e nem sempre há alguém que possa prover informações. Por isso, mesmo que as informações sejam confidenciais *a priori*, a vida do paciente obviamente deve ser priorizada e os profissionais devem ter acesso a elas. Como este caso bem ilustra, é necessário ter um sistema de controle de acessos que seja consistente e flexível.

- Armazenamento de dados: as instituições devem atender a *constraints* específicos de armazenamento de dados clínicos, estabelecidos por padrões (e.g., DICOM para imagens médicas) e pelas exigências impostas pela legislação para a proteção de dados pessoais.

Tais requisitos podem ser atendidos através das medidas (ou serviços) de segurança, que empregam em sua maioria mecanismos criptográficos, como assinaturas digitais e cifras (Wohlmacher e Pharow, 2000). Existem vários serviços de segurança conhecidos, como autenticidade, integridade, confidencialidade e disponibilidade. Entretanto, há uma grande variação nas definições de cada um deles, ocorrendo freqüentemente situações em que dois serviços acabam sendo redundantes ou com atuações semelhantes (e.g., confidencialidade e privacidade). Bleumer (1995) oferece uma definição distinta de cada serviço, e Kobayashi *et al*. (2004) propõem uma definição mais formal dos serviços mais comuns.

De um modo geral, são cinco os serviços básicos que possuem maior relevância para a área médica (van der Haak *et al*., 2003):

- *confidencialidade*, para que os dados do paciente não estejam disponíveis para pessoas não autorizadas;
- *integridade*, para que os dados não sejam alterados ou ainda apagados de forma indevida;
- *autenticidade*, para que se saiba o autor dos dados e para que a sua identidade seja confirmada;
- *auditabilidade*, para que se possam rastrear as ações tomadas por um usuário;
- *disponibilidade*, para que os dados possam ser acessados e usados por pessoas devidamente autorizadas.

Cabe lembrar que esses serviços trazem consigo outros serviços não menos importantes, tais como o *controle de acesso*, a *privacidade* e a *irrefutabilidade* (também conhecida como não-repudiação).

As suas implementações podem se dar em duas grandes áreas (Blobel e Holena, 1998):

- A segurança da *comunicação*, para que duas entidades confiáveis possam trocar dados de forma confiável;
- A segurança da *aplicação*, para que as funcionalidades e os dados da aplicação possam ser acessados e utilizados de forma controlada e confiável por entidades também confiáveis.

## Implementações de segurança em ambientes de saúde

**Grupos de trabalho em nível nacional e transnacional** – Existem alguns grupos que abordam a segurança em ambientes na área da saúde. O mais conhecido talvez seja a IMIA (*International Medical Informatics Association*), estabelecida formalmente em 1979 para atender a demandas específicas na aplicação da ciência e tecnologia da informação na área da medicina, saúde e pesquisa biomédica. Dentro dessa associação existem inúmeros grupos de trabalho que são especializados em uma determinada área. Um dos grupos é o *Working Group 04* (WG04), que trata especificamente da segurança na área da saúde (IMIA, 2005), que já desenvolveu numerosos trabalhos referentes à proteção de registros eletrônicos do paciente, segurança em comunicação de dados etc.

Paralelamente, a ISO tem um Comitê Técnico (TC) específico para a área de informática em saúde, a ISO/TC215, que trabalha em conjunto com vários grupos, como o DICOM e a IMIA, levando a publicação de guias para a área (Kwak, 2005). Outras iniciativas relativas à segurança podem ser vistas também em grupos de trabalhos de padrões como o DICOM e o HL7.

A Europa lançou várias iniciativas, sendo que uma das mais importantes foi proposta em meados da década de 90: o projeto AIM/SEISMED (*Advanced Informatics in Medicine: Secure Environment for Information Systems in MEDicine*). Este projeto teve o objetivo de levantar e propor guias de instruções que iam desde o nível mais abstrato, definido pelo código de deontologia (ética e moral), passando pelas políticas de segurança e pelas seguranças de rede, sistemas e bases de dados, até chegar a mecanismos criptográficos. Provê também instruções sobre análise de riscos, implementações técnicas e validação (Bleumer, 1995).

Este projeto foi continuado e validado dentro do âmbito do Projeto ISHTAR (Barber *et al*., 1997), que gerou uma série de ferramentas e materiais de segurança na área da saúde. Estas, por suas vez, propiciaram avanços na área de proteção de dados individuais (Barber, 1998) que foram incorporados em padrões europeus vigentes atualmente (CEN/TC 251, 2005), e que continuam sendo aperfeiçoados através de projetos sobre o tema propostos dentro do programa *eEurope* (eEurope, 2005).

Recentemente, países como o Japão (JAHIS, 2005; Toyoda, 1998), a Malásia (Mohan e Yaacob, 2004) e a Austrália (CSIRO, 2005) também lançaram iniciativas para a segurança das informações em saúde.

No Brasil, é a SBIS (Sociedade Brasileira de Informática em Saúde) quem está mais engajada neste campo, contemplando aspectos de segurança dentro do seu processo de certificação dos Registros Eletrônicos de Saúde (RES), juntamente com o CFM (SBIS, 2004; SBIS, 2005). Dentro desse processo, existem dois níveis de segurança: no primeiro, o RES deve atender a requisitos como autenticação e controle de acesso, controle do fluxo de informação, integridade dos dados, cópias de segurança e sigilo, entre outros. Uma vez atendidos tais requisitos, é possível alcançar o segundo nível, com a introdução adequada de certificados digitais.

**Políticas e gerenciamento em alto nível** – A questão das políticas de segurança na área da saúde é um tema bastante relevante (Anderson, 2000). De um modo geral, as políticas podem ser estabelecidas em um âmbito global ou governamental – seja municipal, estadual ou nacional – e devem refletir as complexas e consistentes estratégias estabelecidas para a segurança, em âmbito local ou institucional, além de estabelecer diretrizes mais pormenorizadas para se adequar às políticas de âmbito global.

O NHS (*National Health Service*) propõe uma abordagem holística que merece destaque, definindo o chamado modelo HORUS, que inclui aspectos como: conferir segurança e confidencialidade à informação; obter informações de forma eficiente e precisa; armazenar informações confiáveis; usar informações de forma efetiva e ética; e compartilhar informações de forma legal e apropriada (Donaldson e Walker, 2004). Isso implica em definição de padrões, leis e portarias regulatórias acerca da qualidade de informação, acesso aos dados do paciente e consentimento esclarecido, entre outros aspectos. Isso será mapeado localmente (ou seja, em cada instituição) em políticas e procedimentos que irão conferir a aderência da instituição às normas de nível mais alto, como ilustra a Figura 5.

Em nível local, Bleumer (1995) defende o uso de uma visão descentralizada para políticas de segurança, que devem explicitar quais entidades (ou grupos de entidades) devem ser capazes de atender a quais requisitos de segurança. A maioria das políticas de segurança atual usa uma visão centralizada, ou seja, explicitam quais grupos devem confiar em quais objetos (e.g., componentes de *software/hardware*) ou indivíduos. Sem isso, a abordagem centralizada assume a existência de um "grande irmão amigável" no qual todo usuário confia, enquanto que a abordagem descentralizada assume agentes colaborativos de usuário, onde cada agente é confiado apenas por seu próprio usuário.

Anderson (1996) define um conjunto de políticas para a segurança nas informações de saúde, que abrange o controle de acesso propriamente dito, a abertura (acesso) de registros, consentimento e notificação, persistência dos dados, atribuição (quem gerou a informação) e fluxo de informações. E mais recentemente, Roger-France (2004) apresenta um caso no qual políticas de gerenciamento do Prontuário Eletrônico do Paciente (PEP) foram estabelecidas dentro de um hospital universitário na Bélgica, de acordo com as diretrizes estabelecidas pelo Conselho de Medicina Belga.

**Arquiteturas e *frameworks* de segurança propostos para a área da saúde** – Apesar de existirem várias implementações de segurança para a saúde, a maioria delas atende a desafios específicos. Existem poucas propostas para arquiteturas e *frameworks* de segurança, especialmente quando comparado com outras áreas como *Internet banking*, na qual existem várias propostas de segurança, como a de Huchinson e Warren (2003).

Uma das primeiras propostas foi uma arquitetura multiestratificada e modular para as informações em saúde, a qual ressalta que a tecnologia sempre estará atrasada no tocante à segurança, e afirma que uma das maiores vulnerabilidades é o uso não-autorizado de recursos por pessoas autorizadas (Essin e Lincoln, 1994). Dentro desta arquitetura, a autenticidade e a integridade dos dados não fazem parte da segurança, que engloba mais a parte de confidencialidade e privacidade.

A Comunidade Européia lançou inúmeros projetos sobre o tema, como TrustHealth e MedSec (MedSec, 1997), que adotaram o uso de componentes para implementar a segurança. Essa abordagem foi utilizada também por Baur *et al*. (1997), com a implementação de uma arquitetura de segurança para tele-radiologia,

| | | | |
|---|---|---|---|
| Responsabilidades em Nível Global | Padrões<br>Legislação<br>Regulação | | |
| Responsabilidades em Nível Local | Acessibilidade<br>Aderência<br>Transparência<br>Direitos | Prontidão<br>Completude<br>Precisão<br>Relevância | Integridade<br>Confidencialidade<br>Disponibilidade<br>Auditabilidade |

**Figura 5.** Modelo de governança da informação. ***Figure 5.*** *Information governance model.*

desde o processo de determinação da política até a implementação de alguns serviços em *software*. A sua modelagem foi feita através de UML (*Unified Modeling Language*), dentro do modelo ODP (*Open Distributed Processing*), com alguns elementos incorporados da iniciativa CORBAMed, que atendem a alguns dos requisitos de segurança na área da saúde (Blobel e Holena, 1998), e que também são utilizados em bibliotecas médicas virtuais (Papadakis *et al*., 2001).

O uso de componentes também foi adotado por Jaeger *et al.* (1998), que propuseram uma arquitetura de segurança baseada em componentes para a implantação de políticas de segurança, de forma a possibilitar uma boa flexibilidade e desempenho relativos à segurança, desvinculando os componentes de segurança das entidades que serão protegidas.

Essa visão de componentes foi posteriormente ampliada para abranger a informação em saúde como um todo, com a proposição de uma modelagem que abarcasse desde políticas até mecanismos, mostrando modelos de informação e casos de uso, dentro do paradigma de *shared care* e de modelo multiestratificado de segurança (Blobel e Roger-France, 2001).

Recentemente, evoluções da visão componentizada estão sendo apresentadas. Uma arquitetura proposta também para a área da saúde é o MDA (*Model-driven architecture*) para permitir interoperabilidade, portabilidade, escalabilidade, flexibilidade e robustez em ambientes distribuídos, como é o caso das informações na área da saúde, em particular os registros eletrônicos do paciente (Blobel, 2006). Mas a arquitetura que vem ganhando maior popularidade é a de *Web Services* e do seu sucessor, o SOA (*Service Oriented Architecture*), cujas funcionalidades são oferecidas através da rede. Para a área da saúde, essa arquitetura se adequa bem dentro da proposta do Registro Eletrônico de Saúde do paciente, mas torna-se necessário lidar com os aspectos de segurança e privacidade dos dados trafegados, o que pode ser feito através da adoção de medidas tecnológicas (Weaver *et al*., 2003; Wimalasiri *et al*., 2005).

Em termos interinstitucionais, existem vários desafios a serem solucionados para um compartilhamento seguro de informações, uma vez que diferentes instituições costumam adotar diferentes políticas de segurança e diferentes implementações tecnológicas. Um dos modelos propostos foi o modelo HARP, que emprega a abordagem de *middleware* de segurança e um servidor TTP (*Trusted Third Party*) com a capacidade de mapeamento de políticas de segurança (Blobel, 2002). Uma outra iniciativa foi proposta pelo projeto MEDITRAV EU, que gerou um registro portável para comunicação interorganizacional (Ruotsalainen e Pohjonen, 2003).

Atualmente existem duas vertentes para a segurança interinstitucional: na primeira existe a integração das plataformas existentes para formar um padrão nacional de segurança, e na segunda existe uma rede difusa *peer-to-peer,* que conecta dinamicamente as diferentes instituições e domínios, com negociação dinâmica de permissões (Ruotsalainen, 2004).

**Implementações de segurança da comunicação** – Grande parte das implementações de segurança da comunicação na área da saúde pode ser considerada como sendo típica, ou seja, com o uso de tecnologias e algoritmos bem conhecidos para segurança dos dados, sem nenhuma característica adicional em termos de implementação, baseando-se na suposição de que a segurança da comunicação independe do tipo de dado trafegado na rede.

Uma das primeiras iniciativas para comunicação segura em saúde foi o Secure Talk 1.0 (Bleumer, 1994), quando ainda não existiam padrões como o DICOM e o HL7. Nestes primórdios, houve até mesmo o desenvolvimento de protocolos específicos de segurança (Makris *et al*., 1997). Depois surgiram alguns trabalhos sobre autorização de acesso em nível de rede para visualização de dados (Malamateniou *et al*., 1998) e propostas de medidas de segurança para comunicação (Al-Salqan, 1998).

A telemedicina e o surgimento do Prontuário

Eletrônico do Paciente levaram à maior disseminação dos mecanismos de segurança de rede, que começaram com abordagens bastante ingênuas (Lees *et al*., 1999) até chegar ao tunelamento com criptografia (Wang, 1999), uso de infra-estrutura de chaves públicas (ICP) e TTP (Takeda *et al*., 2000) ou o emprego simultâneo das duas soluções acima (Hans, 2000), sendo estes os meios mais utilizados atualmente para a segurança no tráfego de dados de um modo geral, incluindo-se a comunicação de dados entre instituições (van der Haak *et al*., 2003). Em particular, a ICP ganhou uma importância grande para a prescrição automática de medicamentos, auxiliando a comunicação entre a instituição de saúde e a farmácia (Song *et al*., 2002), sendo uma das ferramentas para se garantir a privacidade do paciente (Ball *et al*., 2003).

Os trabalhos mais recentes nesta área se atêm menos à implementação do canal seguro de comunicação em si e mais à adição de características mais específicas de segurança, por considerarem que a solução de tunelamento com ICP já é suficiente para prover o canal seguro desejado. Dentre outros trabalhos, pode-se citar a inserção das informações do paciente nas imagens médicas para reduzir o *overhead* de transmissão e armazenamento (Acharya *et al*., 2003), o desenvolvimento de interfaces de usuário para autenticação da comunicação (Josang e Patton, 2003) e para controle e rastreamento de acessos (Reni *et al*., 2004), a interconexão de sistemas de saúde baseados em Web (Gritzalis e Lambrinoudakis, 2004) e a tradução adequada de políticas de segurança em termos de listas de controle de acesso (Lee *et al*., 2005).

A introdução da mobilidade na área da saúde, o chamado *m-health*, abriu novos campos de pesquisa e trouxe desde cedo a preocupação com a sua segurança (Merger *et al*., 1997). Mas foi somente nos últimos anos, com as primeiras instalações e configurações de redes *wireless* para ambientes de saúde (Owens *et al*., 2001) e com a tendência crescente de adoção de dispositivos móveis (Lu *et al*., 2005), que as vulnerabilidades da comunicação em sistemas móveis ganharam maior atenção (Jøsang e Sanderud, 2003). Isso traz consigo novos desafios para a segurança (Istepanian, 2005), tais como a facilidade na interceptação de mensagens e a maior probabilidade de violação da segurança física, com perdas, furtos e roubos de aparelhos (Yu e Yu, 2004). Isso estimulou a criação e implantação de arquiteturas de sistemas móveis para a saúde, levando-se em conta as vulnerabilidades de segurança (Marti *et al*., 2004). Mas ainda não existe nenhuma implantação totalmente validada para a mobilidade na área da saúde.

Um ramo específico para a saúde que deve ser mencionado é o monitoramento remoto de pacientes, como por exemplo, o caso em que pessoas em idade avançada, ou crianças com doenças crônicas, com saúde suficiente para não necessitarem internação, mas que precisam de um acompanhamento contínuo em seus lares (Kuo *et al*., 2003). Alguns estudos foram desenvolvidos para se implantar segurança nas comunicações entre a casa dos pacientes e a instituição de saúde, tanto na segurança dos dados em si do canal de comunicação (Kara, 2001) quanto na segurança de plataformas mais sofisticadas para teleconferência com espaços colaborativos (Starida *et al*., 2003).

**Segurança da aplicação**

**Integridade e Autenticidade** – Em termos de integridade e autenticidade, as informações que melhor devem ser protegidas são as imagens médicas, que são dados de alta complexidade e de elevada importância para o diagnóstico, tratamento e pesquisa. Existem duas grandes vertentes para garantir esses dois serviços de segurança: o armazenamento das informações de integridade e autenticidade embutidas na imagem, através do uso de marcas d'água, e fora da imagem (e.g., no seu cabeçalho).

A marca d'água consiste em inserir determinadas informações dentro da própria imagem, de forma a permitir sua autenticação (Memon e Wong, 1998). Em particular, as informações acerca da própria imagem podem ser utilizadas como marca d'água para a integridade (Li *et al*., 2000).

Atualmente existem várias técnicas para marca d'água (Albanesi *et al*., 2001) com robustez variável (Liu e Qiu, 2002; Nikolaidis *et al*., 2001), cujas vulnerabilidades podem ser analisadas e reduzidas através de estudos adequados (Barreto e Kim, 1999; Barreto *et al*., 2002).

Entretanto, apesar desta técnica ser bastante conhecida e utilizada em várias aplicações, o seu uso em imagens médicas é bastante recente e ainda não é estabelecido nem reconhecido por padrões como o DICOM, embora existam estudos nos quais se reporta a aplicação de marcas d'água em imagens DICOM (Zain *et al*., 2004; Zhou *et al*., 2001).

Dentre as várias técnicas propostas, como o mascaramento visual e seqüências pseudo-ruidosas (Zhu *et al*., 1996), chaves assimétricas (Wong, 1998), funções de espalhamento (Fridrich e Goljan, 2000) e *wavelets* (Chen *et al*., 2003), existem dois ramos predominantes: o uso de envelope digital como marca d'água (Zhou

*et al*., 2001), onde é gerada uma assinatura digital da imagem que é armazenada de forma criptografada na imagem (Cao *et al*., 2003; Huang, 2004) e o uso de *wavelets* para marcar digitalmente a imagem (Giakoumaki *et al*., 2004).

O uso da marca d'água ainda sofre resistência, pois implica necessariamente em uma adulteração da imagem, ainda que minimamente perceptível. Além disso, os aspectos de desempenho e de usabilidade ainda carecem de melhoria.

A outra vertente é o armazenamento fora da imagem, representada pelo padrão DICOM, em especial a Parte 15 (NEMA, 2004). Neste caso, a imagem é assinada digitalmente e a assinatura é armazenada de forma específica no cabeçalho. Existem algumas implementações comerciais do padrão, mas nem todas as modalidades conseguem transmitir as imagens com segurança, levando ao desenvolvimento de uma "caixa preta" que assina as imagens de acordo com o padrão DICOM (Kroll *et al*., 2003). Um outro uso da assinatura digital foi proposto para laudos, com ênfase na integridade e não na autoria dos dados (Ferreira *et al*., 2004).

**Confidencialidade** – A confidencialidade em nível de aplicação é algo ainda pouco explorado. A ênfase ainda está em termos de comunicação, e a confidencialidade da aplicação normalmente é transferida para sistemas como os bancos de dados.

No caso específico de imagens, a criptografia das informações do paciente está prevista em padrões como o DICOM, mas geralmente as implementações são feitas apenas para proteger as informações do cabeçalho e não a imagem em si (Bernarding *et al*., 2001). Uma outra alternativa envolve a utilização de imagens inócuas para armazenar dados do paciente (Miaou *et al*., 2000; Chao *et al*., 2002).

**Auditabilidade** – A auditabilidade, que é a propriedade de rastrear as ações tomadas pelos usuários, é extremamente importante dentro do âmbito legal para que se possa determinar a responsabilidade do usuário, sendo geralmente implantada através da geração e armazenamento de um *log*.

Não há muitas iniciativas para este serviço de segurança dentro da área da saúde. Dois trabalhos que merecem nota são: o desenvolvimento de um *hardware* seguro, que criptografa os *logs* para melhorar a sua confidencialidade e reduzir as chances de serem adulterados (Ferreira *et al*., 2003) e a proposta de uma arquitetura para um PACS (*Picture Archiving and Communication System*) com ênfase especial na auditoria, com camadas para registrar as ações tomadas pelo usuário (Liu *et al*., 2005).

**Controle de Acesso** – Em um ambiente de saúde, o controle de acesso é de suma importância, sendo relacionado à *privacidade* (discutida posteriormente) para evitar que pessoas não autorizadas possam manipular dados dos pacientes. Entretanto, o acesso é algo que necessita de muita flexibilidade. Por exemplo, um clínico normalmente não tem acesso aos dados de um paciente associado a um outro médico, mas em um caso de emergência, ele deve ter permissão para a visualização.

Assim, a especificação das políticas de acesso é algo fundamental, já que deve ser expresso de uma forma que seja facilmente mapeável em um conjunto de diretrizes lógicas. Para a área da saúde, foram lançadas algumas propostas, sendo que a mais recente é o uso de lógica temporal linear de primeira ordem, para modelar conceitos como delegação e permissão, através da definição de condições de contorno para o fluxo, baseadas na ordem com que as operações são realizadas (Sohr *et al*., 2005).

Uma outra área de pesquisa é a proposta dos modelos de acesso. Para um controle eficaz de acesso, a solução mais aceita atualmente é o controle de acesso baseado em papéis (*Role Based Access Control*), apesar de existirem soluções mais triviais, com o uso de banco de dados relacionais (Pereira *et al*., 2001). Zhang *et al.* (2002) introduziram a questão da delegação de papéis para o controle de acesso, expandido por Motta e Furuie (2003), que propuseram um modelo baseado em papéis que leva em consideração o contexto, sendo um dos poucos trabalhos sobre este campo na área da saúde. Mais recentemente, um modelo de acesso interinstitucional foi proposto na Austrália, levando em conta a atribuição, revogação, transporte e conteúdo dos papéis (Dalley *et al*., 2005).

A terceira área de pesquisa compreende as formas de implementação (*enforcement*) da política. A proposta mais relevante é o uso de segurança em *tags* XML para introduzir o conceito de controle de acesso e lançar mão dos recursos de segurança do XML dentro de uma arquitetura multi-agente para o prontuário eletrônico (Wimalasiri *et al*., 2004). Esse método foi estendido para ser incorporado dentro da proposta da *Service Oriented Architecture* (Wimalasiri *et al*., 2005).

**Identificação** – Certificar-se que o usuário é realmente o usuário que alega ser sempre constituiu um grande desafio em termos de sistemas computacionais. Existem atualmente três métodos para identificação, baseados em algo que o usuário *conhece*, algo que o usuário *possui* e algo que o usuário *é* (Figura 6).

A alternativa mais comum é o uso do conhecimento

do usuário, geralmente um *login* e uma senha. A questão da robustez das senhas e do seu gerenciamento é um desafio a ser tratado, mas que não será discutido no escopo deste artigo.

O método que vem ganhando maior visibilidade é o uso de objetos (*tokens*) que o usuário possui para possibilitar a sua identificação. O item mais comum é o *smart card*, contendo informações do usuário e sua chave. Existe uma implantação de um protótipo de PKI (*Public Key Infrastructure*) na área da saúde com *smart cards* (Takeda *et al*., 2004). Mas outros tipos de *tokens* podem ser usados para que o paciente possa acessar os seus dados (Dalley *et al*., 2005), incluindo-se o uso de transmissores RF para a identificação de pacientes (Cavalleri *et al*., 2004).

O terceiro método é a biometria, que é baseado nas características físicas do usuário, como impressões digitais e padrões da íris. Existem vários meios biométricos com diversas características com relação a aspectos como universalidade (todas as pessoas possuem a característica), distintividade (não existem duas características iguais) e permanência (Delac e Grgic, 2004). Mas para a área clínica, praticamente não há nenhuma pesquisa sobre a sua utilização, aparecendo apenas em um projeto global de segurança (Weaver *et al*., 2003).

**Privacidade**

A privacidade é um motivo crescente de preocupação para muitos. Já em 2000, uma pesquisa realizada nos Estados Unidos apontou que a invasão de privacidade era o principal medo para os anos seguintes (Swire e Steinfeld, 2002). A evolução rápida da tecnologia permite manipulações e distribuições de dados em grande quantidade, demandando políticas e mecanismos tecnológicos para gerenciar e controlar o fluxo de informações sem prejudicar o seu uso. Em particular, o surgimento do conceito de computação ubíqua reforça ainda mais tal demanda (Iachello e Abowd, 2005).

Basicamente, a privacidade consiste na capacidade de controlar a liberação das informações, provendo-as na quantidade correta, para a pessoa correta, no momento certo e na qualidade correta (Wohlmacher e Pharow, 2000), dentro de quatro grandes dimensões para análise (Earp e Payton, 2000):

- Coleção: preocupação de que grandes quantidades de dados pessoais sejam coletados e armazenados;
- Uso não autorizado: preocupação de que a informação coletada seja usada para uma finalidade diferente da original;
- Acesso indevido: preocupação de que os dados possam ser acessados facilmente por pessoas sem a devida permissão para tal;
- Erros: preocupação sobre a introdução de erros acidentais e/ou deliberados nos dados pessoais.

Para a área da saúde, a perda de informações e os problemas de privacidade e confidencialidade do paciente são uma ameaça real. No NHS CRS (*National*

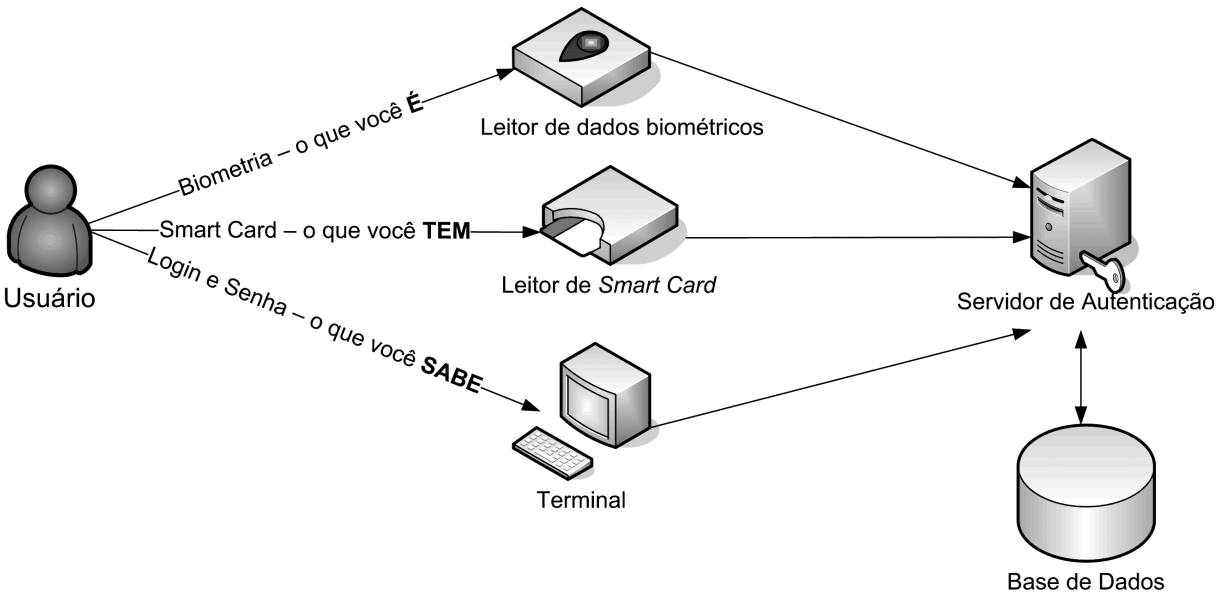


**Figura 6.** Formas de identificação do usuário. ***Figure 6.*** *Ways of user identification.*

*Health System Care Records Service*), praticamente não é possível controlar a liberação das suas informações a terceiros (Lettice, 2005). Existem relatos de casos em que houve perda de informações confidenciais de milhares de pessoas (Oates, 2005).

Este problema se torna mais crítico em grandes estruturas de informação em saúde. Neste caso, questões como a liberação de dados demográficos do paciente e a ligação com os dados disponíveis, a visualização de resultados de exames sem ter o consentimento explícito do paciente e a questão da mineração de dados sem identificar cada paciente passam a ter um peso extremamente relevante (Neame e Olson, 2004).

Atualmente há uma facilidade grande para a violação da privacidade, com a liberação e obtenção indiscriminada de dados, aliada às políticas de privacidade mais direcionadas a camuflar as brechas e proteger as empresas contra eventuais ações legais do que proteger o usuário propriamente dito (Schwaig *et al*., 2005). Com isso, tende a aumentar cada vez mais a pressão por parte da legislação e das pessoas para que exista um maior controle sobre a privacidade.

Assim sendo, os profissionais de TI devem implementar medidas de segurança e gerenciamento adequado de dados com dois objetivos principais: proteger dados vitais da organização e também as informações pessoais do usuário contra liberações não autorizadas. Para tanto, é necessário a criação de uma arquitetura voltada para a privacidade, que leve em conta fatores como:

- O desenvolvimento de uma solução integrada, que se adapte ao ambiente heterogêneo da instituição;
- A separação da privacidade da aplicação em si, para evitar que os aplicativos tenham que ser modificados para proteger o paciente;
- O suporte a granularidades diferentes de políticas de privacidade;
- A possibilidade de lidar com dados estruturados e não-estruturados de forma apropriada;
- A flexibilidade para se adequar a diferentes aspectos das políticas de privacidade.

Este campo de pesquisa tem propostas bastante recentes, como uma arquitetura para a privacidade, que inclui a criação, implementação, *enforcement* e auditoria das políticas de privacidade, identifica as necessidades da organização e propõe um *framework* usável para gerenciamento simples e flexível de políticas de segurança (Brodie *et al*., 2005) e uma arquitetura com o uso de agentes para implementar políticas de privacidade, que apresenta uma divisão clara entre os consumidores e os provedores de serviços de privacidade, facilitando a implementação e manutenção (Yee e Korba, 2005).

Além disso, deve-se levar em consideração fatores como o gerenciamento de informações em bases de dados distribuídos e fragmentados, o controle do prontuário em papel e a implementação da segurança em conjunto com esquemas melhores de gerenciamento das bases de dados (Lederman, 2004). Em particular, a proteção da base de dados contra o uso indevido é algo que merece destaque (Peterson, 2002; Olivier, 2002), e a maioria das pesquisas segue esta linha. Alguns trabalhos que podem ser citados são a utilização de linguagem XML para a definição de políticas de privacidade com o uso de P3P (*Platform for Privacy Preferences*) ou EPAL (*Enterprise Privacy Authorization Languages*) para as bases de dados (Agrawal *et al*., 2004), a introdução de uma solução baseada em visões de banco de dados que mapeiam regras de privacidade (Yee e Korba, 2004) e uma proposta envolvendo alterações dinâmicas feitas nas pesquisas em bases de dados, de forma que a pesquisa seja feita com restrições de privacidade, mas de forma transparente ao usuário (Power *et al*., 2005).

**O cenário nacional**

O Brasil ainda contribui de forma extremamente modesta na área da segurança em informações na área da saúde. Existem propostas dentro de projetos específicos, como o TISS (Troca de Informação em Saúde Suplementar), em que a segurança se baseia nas normas do Conselho Regional de Medicina (CRM) (TISS, 2006), do Cartão Nacional de Saúde, em que se utiliza VPN (*Virtual Private Networks*) e SSL (*Secure Socket Layer*) para a segurança da comunicação (DataSUS, 2006). Existe ainda a proposta da ANVISA (Agência Nacional de Vigilância Sanitária), onde há o uso da assinatura digital (Mussi, 2005).

Na área acadêmica, merece destaque a solução para controle contextual de acesso (Motta e Furuie, 2003). Os autores propuseram um modelo baseado em papéis, com flexibilidade através do conceito de autorizações fortes e fracas, que permite que um mesmo usuário receba dinamicamente permissões diferentes de acordo com a situação. Por exemplo, o modelo permite a implantação de uma política na qual um médico tenha acesso a um conjunto completo de dados do paciente durante o seu expediente; mas se o mesmo médico tentar visualizar em sua casa os dados do mesmo paciente, ele vai ter acesso a um conjunto bem mais restrito de dados. Entretanto, se o médico for o responsável pelo paciente, então se pode permitir

que ele continue tendo acesso aos dados completos do paciente mesmo em casa.

Uma outra vertente de pesquisa está sendo abordada pelo grupo de trabalho dos autores deste artigo. O foco desta vertente está na área de segurança de imagens médicas, produzindo trabalhos que vão desde o levantamento de requisitos (Kobayashi *et al*., 2004), à elaboração de uma arquitetura para segurança fim-a-fim de imagens médicas (Kobayashi e Furuie, 2004) e alguns resultados preliminares acerca da sua implementação (Kobayashi *et al*., 2005).

## Discussão

Foi apresentado um panorama geral da segurança em informações médicas em vários níveis, desde os aspectos de arquiteturas e *frameworks* gerais até implementações mais específicas.

Pode-se dividir os trabalhos em duas grandes áreas: a área de iniciativas em âmbito regional, nacional ou transnacional, onde são desenvolvidas infra-estruturas de grande porte para a segurança, e a outra que abarca iniciativas direcionadas para resolver um aspecto bastante pontual.

A primeira área costuma receber incentivos governamentais e busca oferecer uma solução completa para a segurança. Tem por objetivo fornecer soluções e implementações padrão, bem como servir de base para eventuais padronizações e legislações. Devido à complexidade e heterogeneidade do cenário, ainda não há um *framework* bem consolidado que tenha sido adotado de forma única por todas as instituições de um país. Tampouco há essa tendência, preferindo-se adotar um modelo evolutivo para integrar as diferentes soluções, utilizando-se uma visão *bottom-up* ao invés de *top-down*.

Um aspecto importante a ser destacado é a questão da modelagem. Muitos dos padrões e implementações de modelos existentes dão uma dimensão apenas secundária à segurança, dificultando a sua representação dentro das metodologias estabelecidas, em particular as do HL7 (*Health Level 7*) e do JAHIS (*Japanese Association of Healthcare Information System Industry*) (Fernandez e Sorgente, 2005). Assim, na situação atual, a implantação de segurança atendendo aos padrões ainda é um processo bastante complexo, que necessita aperfeiçoamentos nos próprios padrões para facilitar a criação de ambientes seguros.

A segunda área é mais acadêmica, e visa resolver desafios localizados. A grande maioria dos trabalhos oferece soluções que incorporam pouca ou nenhuma visão geral das informações médicas, o que pode prejudicar ou até mesmo impedir a sua introdução efetiva em um ambiente de produção. Existem inúmeras pesquisas na área de segurança de um modo geral, as quais geram resultados que podem ser empregados também à área da saúde. A utilização dos resultados dessas pesquisas na área médica necessita, entretanto, de validação e de adaptações. Existem também muitos serviços que são oferecidos por implementações comerciais, que atendem a alguns requisitos. Deve-se manter isso em mente quando da pesquisa, para evitar abordar problemas já resolvidos.

Com relação a iniciativas nacionais, elas ainda estão extremamente incipientes, existindo um espaço bastante amplo para a realização de pesquisas. Além disso, com a disseminação dos Sistemas de Informação Hospitalar pelo território nacional, prevê-se o surgimento de uma demanda por soluções condizentes com o cenário nacional e por recursos humanos para a área.

Por outro lado, ainda faltam legislações e diretrizes específicas em âmbito nacional para direcionar melhor as iniciativas de segurança, principalmente em termos de privacidade. Um exemplo é o acesso irrestrito do paciente às suas informações. Na situação atual, não existe nenhuma lei que assegure explicitamente esse direito no Brasil, sendo uma concordância tácita apenas.

Existem alguns aspectos adicionais interessantes, que serão discutidos a seguir.

**Do prontuário do *médico* para o prontuário do *paciente*** – Atualmente, existe a tendência cada vez maior de considerar o prontuário como sendo do paciente e não do médico, que era a visão comum até algumas décadas atrás. Essa diferença na visão se traduz na unificação de todas as informações do paciente, de forma que este possa ter um acesso irrestrito às suas informações, como lhe é garantido por lei em alguns países. No caso do Brasil, ainda não há uma legislação específica, como já foi apontado.

Entretanto, a *guarda* dos dados do paciente é algo que deve ser analisado com cuidado. Se a guarda passar totalmente para a responsabilidade do paciente, para que este tenha acesso permanente aos seus dados, isso pode trazer uma série de conseqüências prejudiciais em termos de segurança (Anderson, 1996). Por outro lado, se as várias instituições forem as responsáveis pela guarda, nem sempre o paciente poderá ter acesso aos seus dados de forma imediata, especialmente no caso de informações distribuídas por vários estabelecimentos. Além disso, existe o risco do uso dos seus dados pessoais para fins como mineração de dados, podendo ser uma fonte de ameaças para a sua privacidade.

A solução mais adotada é um compromisso entre os pacientes e as instituições, de forma que estas serão responsáveis pela guarda das informações, mas com a adoção de uma série de políticas, procedimentos e mecanismos para garantir a segurança dos dados e evitar seu uso indevido.

Esta discussão está diretamente relacionada com a questão da *privacidade*, apresentada anteriormente.

**Armazenamento por longo prazo de registros eletrônicos de saúde** – O armazenamento de registros médicos, seja em papel ou em formato eletrônico, é ditado pelas leis arquivísticas brasileiras, que estabelecem uma guarda bastante longa dos registros. Por exemplo, o prontuário de um servidor do Ministério Público Federal deve ser mantido durante 100 anos ao total (Ministério Público Federal, 2005). No caso de registros em formato eletrônico, muitas vezes o armazenamento é por tempo indeterminado. Para prontuários médicos em suporte de papel, o prazo mínimo estabelecido é de 20 anos no Brasil (Conselho Federal de Medicina, 2002).

O Conselho Federal de Medicina estabeleceu uma série de procedimentos para o armazenamento por longos períodos (Conselho Federal de Medicina, 2002) e é interessante ter uma visão geral dos pontos chave que devem ser levados em consideração, já que este tópico faz parte da segurança das informações do paciente. Luz (2004) apresenta um estudo do PEP sob o ponto de vista arquivístico. Os requisitos básicos são, obviamente, a *integridade* e a *autenticidade* dos registros. Em outras palavras, os dados corretos devem ter sido armazenados de forma correta e recuperados apropriadamente através de um processamento para exibir uma reprodução íntegra e autêntica do registro.

Existem cinco fatores adicionais que devem ser levados em consideração para o armazenamento dos registros por tempo indeterminado (Waugh *et al*., 2000):

- Encapsulamento: a informação é preservada juntamente com metadados que a descrevem;
- Autodocumentação: a informação pode ser compreendida e analisada sem a necessidade de documentos externos;
- Auto-suficiência: há uma dependência mínima com relação a sistemas, dados ou documentos;
- Documentação do conteúdo: é possível a um usuário futuro encontrar ou implementar ferramentas para visualizar a informação preservada;
- Preservação organizacional: a informação é armazenada de forma que a organização é de fato capaz de utilizá-la para os seus objetivos.

Para atender a estes pontos, existem iniciativas para preservação dos registros, que podem ser divididas em cinco grandes categorias (Lin *et al*., 2003):

- Preservar a tecnologia original utilizada;
- Emular a tecnologia original nas plataformas mais recentes;
- Migrar a tecnologia para recuperar e utilizar os registros;
- Migrar os registros em si para formatos mais atuais;
- Converter os registros para formas padronizadas.

No caso de registros em saúde, há uma tendência para a padronização das informações. Entretanto, deve-se lembrar que nem todas as informações em saúde possuem padrões associados, e o próprio processo de padronização possui vantagens e desvantagens.

**A questão do anonimato** – O anonimato é uma característica bastante importante para a manutenção da *privacidade* dos dados, já que a não identificação dos dados dificulta ou até mesmo impede a sua associação com o paciente. Em um ambiente como o de saúde, onde há um compartilhamento vasto de informações, o anonimato permite um controle melhor sobre a coleção e a inferência de conhecimento.

Deve-se manter em mente que o anonimato não é simplesmente ocultar ou eliminar o nome do paciente. Por exemplo, é possível determinar o paciente através de dados como a idade, o sexo e a data de alta do hospital. Um outro exemplo: é possível identificar uma mulher em uma dada população a partir da data de nascimento de dois de seus filhos. E a integração com outros sistemas pode facilitar ainda mais a identificação (Bertino *et al*., 2005). Por isso, torna-se necessário desenvolver mecanismos de anonimato, ressaltando que qualquer aspecto de segurança deve estar refletido em políticas, procedimentos e mecanismos, além de atender à legislação vigente.

Sob o ponto de vista tecnológico, existem três níveis de anonimização (El-Kalam *et al*., 2004):

- Reversível: os dados são criptografados, e podem ser sempre recuperados através de uma chave;
- Irreversível: os dados são adulterados de forma que não mais podem ser recuperados. É o caso mais intuitivo de anonimato. Um exemplo desse tipo de processamento é o uso das funções de *hash* ou de espalhamento;
- Inversível: também conhecido como pseudonimização, envolve a adulteração dos dados de forma que seja impossível a reidentificação do paciente, exceto através de um procedimento especial, restrito a uma autoridade altamente confiável.

Existem diversos algoritmos de anonimato, como

generalização e supressão (Bertino *et al*., 2005), o uso de assinaturas em grupo (Ateniese e de Medeiros, 2002) e uma proposta de procedimento genérico para anonimização de dados (El-Kalam *et al*., 2004).

A escolha da solução depende obviamente dos requisitos impostos e a implementação deve levar em consideração os seguintes aspectos:

- O tipo de solução desejado, em termos de procedimentos e mecanismos;
- A pluraridade, se o anonimato deve ser simples, duplo ou até mesmo em múltiplos níveis;
- A interoperabilidade da solução, em particular se o anonimato for implementado ao longo de diversos sistemas em separado. Neste caso, deve-se analisar se é necessário que existam formas de tradução dos meios de anonimato entre diferentes sistemas ou se o mais adequado é implantar um sistema único de anonimato.

Além disso, deve-se analisar a robustez da implementação, em particular nos aspectos de:

- Robustez à reversão, analisando a complexidade de se inverter a função de anonimização;
- Robustez à inferência, levantando-se a dificuldade em se recuperar a identidade da pessoa através de inferências ou de outros métodos indiretos.

## Conclusão

Na sociedade digital moderna, a segurança é um dos valores mais importantes. A proteção dos dados pessoais sensíveis, como os registros eletrônicos de saúde do paciente, é um fator crucial para o bom uso da infra-estrutura da tecnologia de informação.

Desta forma, todos os atores envolvidos no contexto da informação em saúde devem aplicar adequadamente as políticas, procedimentos e mecanismos tecnológicos de segurança para que as informações sejam acessadas e manipuladas de forma controlada.

Há inúmeros serviços de segurança, que podem ser tratados individualmente ou em conjunto, dentro de arquiteturas projetadas para este fim. Para a área médica existem diversos trabalhos realizados, com propostas que variam desde *frameworks* abrangentes até implementações bastante específicas. Mesmo assim, a área da segurança da informação em saúde ainda é bastante incipiente, permitindo pesquisas maiores e mais aprofundadas. Em particular, praticamente não há pesquisa nesta área dentro do Brasil, o que a torna uma linha promissora tanto em termos acadêmicos quanto em termos de mercado, pois permitirá o desenvolvimento de produtos originais que atendam à realidade nacional.

## Agradecimentos

Os autores deste trabalho agradecem ao CNPq pelo auxílio financeiro.

## Referências

Acharya, U.R., Subbanna, B.P., Kumar, S., Min, L.C. (2003), "Transmission and storage of medical images with patient information", *Computers in Biology and Medicine*, v. 33, n. 4, p. 303-310.

Agrawal, R., Kini, A., LeFevre, K., Wang, A., Xu, Y., Zhou, D. (2004), "Managing healthcare data hippocratically", In: *SIGMOD Conference 2004*, Paris, p. 947-948, 13-18 Jun.

Al-Salqan, Y.Y. (1998), "Security and confidentiality in healthcare informatics", In: *Proceedings on 7th Workshop on Enabling Technologies, Infrastructure for Collaborative Enterprises* [*WET ICE'98*], California, p. 371-375, 17-19 Jun.

Albanesi, M.G., Ferretti, M., Guerrini, F.A. (2001), "Taxonomy for image authentication techniques and its application to the current state of the art", In: *Proceedings on 11th International Conference on Image Analysis and Processing*, Palermo, p. 535-540, 26-28 Sep.

Anderson, J.G. (2000), "Security of the distributed electronic patient record: a case-based approach to identifying policy issues", *International Journal of Medical Informatics*, v. 60, p. 111-118.

Anderson, R.J. (1996), "Security in clinical information systems", In: http://www.cl.cam.ac.uk/~rja14/Papers/policy11.pdf.

Associação Médica Mundial (2004), "Declaração de Lisboa, sobre os direitos do paciente. Adotada pela 34ª Assembléia Geral da Associação Médica Mundial em Lisboa, Portugal, setembro/outubro de 1981 e emendada pela 47ª Assembléia Geral da Associação Médica Mundial em Bali, Indonésia, setembro de 1995", In: www.dhnet.org.br/direitos/codetica/medica/14lisboa.html, acessado em 03 de junho de 2004.

Associação Médica Mundial (2004a), "Declaração de Munique, sobre o uso do computador em medicina. Baseada em Resolução adotada pela 27ª Assembléia Geral da Associação Médica Mundial, Munique, República Federal da Alemanha, outubro de 1973 e emendada pela 35ª Assembléia Geral da Associação Médica Mundial em Veneza, Itália, outubro de 1983", In: www.dhnet.org.br/direitos/codetica/medica/19munique.html, acessado em 03 de junho de 2004.

Associação Médica Mundial (2004b), "Declaração de Tel Aviv, sobre responsabilidades e normas éticas na utilização da telemedicina. Adotada pela 51ª Assembléia Geral da Associação Médica Mundial em Tel Aviv, Israel, em outubro de 1999", In: www.dhnet.org.br/direitos/codetica/medica/27telaviv.html, acessado em 03 de junho de 2004.

Ateniese, G., de Medeiros, B. (2002), "Anonymous EPrescriptions", In: *Proceedings of the ACM Workshop on Privacy in the Electronic Society* [*WPES'02*], Washington, p. 19-31, 21 Nov.

Bali, R.K., Feng, D.D., Burstein, F., Dwivedi, A.N. (2005), "Guest Editorial: Introduction to the Special Issue on Advances in Clinical and Health-Care Knowledge Man-

agement", *IEEE Transactions on Information Technology in Biomedicine*, v. 9, n. 2, p. 157-161.

Ball, E., Chadwick, D.W., Mundy, D (2003), "Patient privacy in electronic prescription transfer", *IEEE Security & Privacy Magazine*, v. 1, n. 2, p. 77-80.

Barber, B. (1998), "Patient data and security: an overview", *International Journal of Medical Informatics*, v. 49, p. 19-30.

Barber, B., Louwerse, K., Davey, J. (1997), "White paper on health care information security", *Implementing Secure Healthcare Telematics Applications in Europe* [ISHTAR], Sep.

Barreto, P.S.L.M., Kim, H.Y. (1999), "Pitfalls in public key watermarking", In: *Proceedings of the XII Brazilian Symposium on Computer Graphics and Image Processing* [*SIBGRAPI'99*], Campinas, p. 241-242, 17-20 Oct.

Barreto, P.S.L.M., Kim, H.Y., Rijmen, V. (2002), "Toward secure public-key blockwise fragile authentication watermarking", *IEE Proceedings on Vision, Image & Signal Processing*, v. 149, n. 2, p. 57-62.

Baur, H.J., Engelmann, U., Saurbier, F., Schröter, A., Baur, U., Meinzer, H.P. (1997), "How to deal with security issues in teleradiology", *Computer Methods and Programs in Biomedicine*, v. 53, p. 1-8.

Bernarding, J., Thiel, A., Grzesik, A. (2001), "A JAVA-based DICOM server with integration of clinical findings and DICOM-conform data encryption", *International Journal of Medical Informatics*, v. 64, p. 429-438.

Bertino, E., Ooi, B.C., Yang, Y., Deng, R.H. (2005), "Privacy and ownership preserving of outsourced medical data", In: *Proceedings of the 21st International Conference on Data Engineering* [*ICDE 2005*], Tokyo, p. 521-532, 05-08 Apr.

Biskup, J., Bleumer, G. (1996), "Cryptographic protection of health information: cost and benefit", *International Journal of Biomedical Computing*, v. 43, n. 1-2, p. 61-67.

Bleumer, G. (1995), "Introduction to the SEISMED Guidelines", In: *AIM (Advanced Informatics in Medicine) - Secure Environment for Information Systems in MEDicine - SEISMED (A2033)*, 16 p., Jul.

Bleumer, G. (1994), "Security for decentralized health information systems", *International Journal of Biomedical Computing*, v. 35, n. 1, p. 139-145.

Blobel, B. (2000), "Advanced tool kits for EPR security", *International Journal of Medical Informatics*, v. 60, p. 169-175.

Blobel, B. (2006), "Advanced and secure architectural EHR approaches", *International Journal of Medical Informatics*, v. 75, n. 3-4, p. 185-190.

Blobel, B. (2002), *Analysis, Designs and Implementation of Secure and Interoperable Distributed Health Information Systems*, Studies in Health Technology and Informatics (series), v. 89, Amsterdam: IOS Press.

Blobel, B., Holena, M. (1998), "CORBA security services for health information systems", *International Journal of Medical Informatics*, v. 52, p. 29-37.

Blobel, B., Roger-France, F. (2001), "A systematic approach for analysis and design of secure health information systems", *International Journal of Medical Informatics*, v. 62, p. 51-78.

Brasil (1994), *Portaria do Ministério da Saúde nº 1.286 de 26/10/93- art. 8º e nº 74 de 04/05/94*.

Brasil (2001), *Constituição da República Federativa do Brasil*, São Paulo: Saraiva.

Brasil (2001b), *Novo Código Civil Brasileiro – art. 225*, 2001.

Brasil (2003), *Projeto de Lei PL-20/2003, 2003. Estabelece o Código Nacional de Direitos dos Uusários das Ações e dos Serviços de Saúde e dá outras providências,* In: www.camara.gov.br/sileg/Prop_Detalhe.asp?id=104343, acessado em 31 de maio de 2004.

Brodie, C., Karat, C.M., Karat, J., Feng, J. (2005), "Usable security and privacy: a case study of developing privacy management tools", In: *Proceedings of the Symposium On Usable Privacy and Security* [*SOUPS 2005*], Pittsburgh, p. 35-43, 06-08 Jul.

Cao, F., Huang, H.K., Zhou, X.Q. (2003), "Medical image security in a HIPAA mandated PACS environment", *Computerized Medical Imaging and Graphics*, v. 27, p. 185-196.

Cavalleri, M., Morstabilini, R., Reni, G. (2004), "A wearable device for a fully automated in-hospital staff and patient identification", In: *Proceedings of the 26th Annual International Conference of the IEEE EMBS*, San Francisco, p. 3278-3281, 01-05 Sep.

Cavalli, E., Mattasoglio, A., Pinciroli, F., Spaggiari, P. (2004), "Information security concepts and practices: the case of a provincial multi-specialty hospital", *International Journal of Medical Informatics*, v. 73, n. 3, p. 297-303.

CEN/TC 251 (2005), "European Standards in Health Informatics", In: www.centc251.org/FinWork/greensheetpwd.htm, acessado em 13/12/2005.

Chao, H.M., Hsu, C.M., Miaou, S.G. (2002), "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records", *IEEE Transactions on Information Technology in Biomedicine*, v. 6, n. 1, p. 46-53.

Chen, C.C., Fan, K.C., Wang, S.W. (2003), "A wavelet-based public key image authentication watermarking", In: *Proceedings of the IEEE 37th Annual 2003 International Carnahan Conference on Security Technology*, p. 321-324, 14-16 Oct.

Cintra, L.P. (2004), "Da responsabilidade civil dos estabelecimentos de saúde", In: http://jus2.uol.com.br/doutrina/texto.asp?id=2458, acessado em 03 de junho de 2004.

Conselho da Europa (2004), "Convenção para a Proteção dos Direitos do Homem e da Dignidade do Ser Humano face às Aplicações da Biologia e da Medicina: Convenção sobre os direitos do Homem e a Biomedicina. Adotada e aberta à assinatura em Oviedo, a 4 de Abril de 1997. Entrada em vigor na ordem internacional: 1 de Dezembro de 1999", In: www.dhnet.org.br/direitos/sip/euro/principaisinstrumentos/16.htm, acessado em 03 de junho de 2004.

Conselho Federal de Medicina (1988), "Código de Ética Médica", In: *Resolução CFM nº 1.246/1988*.

Conselho Federal de Medicina (2002), "Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico", In: *Resolução CFM nº 1.639/2002*.

Conselho Regional de Medicina do Estado de São Paulo (2001), "Manual de Princípios Éticos para Sites de Medicina e Saúde na Internet" In: *Resolução CREMESP nº 97/2001*.

CSIRO (2005), "Security and Privacy Health Data Integration (HDI) project", In: http://www.csiro.au/science/psyy.html, acessado em 13/12/2005.

Cushman, R. (1996), "Information and medical ethics: protecting patient privacy", *IEEE Technology and Society*

*Magazine*, v. 15, n. 3, p. 32-39.

Dalley, A., Fulcher, J., Bomba, D., Lynch, K., Feltham, P. (2005), "A technological model to define access to electronic clinical records", *IEEE Transactions on Information Technology in Biomedicine*, v. 9, n. 2, p. 289-290.

DataSUS (2006), "Cartão Nacional da Saúde", In: http://tecnoper.datasus.gov.br/Apresentacoes/01%20-%20HYC%20-%20CNS%20Apresentacao%20Geral.ppt, acessado em 03 de fevereiro de 2006.

Delac, K., Grgic, M. (2004), "A survey of biometric recognition methods", In: *Proceedings of the 46th International Symposium Electronics in Marine* [*ELMAR-2004*], Zagreb, p. 184-193, 16-18 Jun.

Dinklo, J.A. (1974), "Confidentiality of medical data in the usage of data banks", In: *Proceedings of the 1st World Conference on Medical Informatics* [*MEDINFO 74*], Stockholm, p. 181-187, 5-10 Aug.

Donaldson, A., Walker, P. (2004), "Information governance - a view from the NHS", *International Journal of Medical Informatics*, v. 73, n. 3, p. 281-284.

Dwivedi, A., Bali, R.K., Belsis, M.A., Naguib, R.N.G., Every, P., Nassar, N.S. (2003), "Towards a practical healthcare information security model for healthcare institutions", In: *Proceedings of 4th International IEEE Conference on Information Technology Applications in Biomedicine*, Birmingham, p. 114-117, 24-26 Apr.

Earp, J.B., Payton, F.C. (2000), "Dirty laundry: privacy issues for IT professionals", *IEEE IT Professional*, v. 2, n. 2, p. 51-54.

eEurope (2005), "eHealth - Best Practices - Ongoing Projects", In: http://europa.eu.int/information_society/eeurope/ehealth/best_practices/ongoing_projects/index_en.htm, acessado em 13/12/2005.

El-Kalam, A.A., Deswarte, Y., Trouessin, G., Cordonnier, E. (2004), "A generic approach for healthcare data anonymization", In: *Proceedings of the ACM Workshop on Privacy in the Electronic Society* [*ACM WPES'04*], Washington, DC, p. 31-33, 28 Oct.

Essin, D.J., Lincoln, T.L. (1994), "Healthcare information architecture: elements of a new paradigm", In: *Proceedings of the Workshop on New Security Paradigms* [*NSPW '94*], White Point Beach, Nova Scotia, p. 32-41, 20-23 Sep.

Fernandez, E., Sorgente, T. (2005), "An analysis of modeling flaws in HL7 and JAHIS", In: *Proceedings of the ACM Symposium on Applied Computing*, Santa Fe, p. 216-223, 13-17 Mar.

Ferreira, A., Correia, R., Antunes, L., Palhares, E., Marques, P., Costa, P., da Costa Pereira, A. (2004), "Integrity for electronic patient record reports", In: *Proceedings of the 17th IEEE Symposium on Computer-Based Medical Systems* [*CBMS'04*], Bethesda, p. 4-9, 24-25 Jun.

Ferreira, A., Shiu, S., Baldwin, A. (2003), "Towards accountability for Electronic Patient Records", In: *Proceedings of the 16th IEEE Symposium on Computer-Based Medical Systems* [*CBMS'03*], New York, p. 189-194, 26-27 Jun.

Fridrich, J., Goljan, M. (2000), "Robust hash functions for digital watermarking", In: *Proceedings of the International Conference on Information Technology: Coding and Computing*, Las Vegas, p. 178-183, 27-29 Mar.

Giakoumaki, A., Pavlopoulos, S., Koutsouris, D. (2004), "A multiple watermarking scheme applied to medical image management", In: *Proceedings of the 26th Annual International Conference of the IEEE EMBS*, San Francisco, p. 3241-3244, 01-05 Sep.

Grimes, S.L. (2004), "Medical Device Security", In: *Proceedings of the 26th Annual International Conference of the IEEE EMBS*, San Francisco, p. 3512-3514, 01-05 Sep.

Gritzalis, D., Lambrinoudakis, C. (2004), "A security architecture for interconnecting health information systems", *International Journal of Medical Informatics*, v. 73, n.3, p. 305-309.

Gritzalis, S., Lambrinoudakis, C., Lekkas, D., Deftereos, S. (2005), "Technical guidelines for enhancing privacy and data protection in modern electronic medical environments", *IEEE Transactions on Information Technology in Biomedicine*, v. 9, n. 3, p. 413-423.

Hamilton, D.L. (1992), "Identification and evaluation of the security requirements in medical applications", In: *Proceedings of the 5th Annual IEEE Symposium on Computer-Based Medical Systems*, Durham, p. 129-137, 14-17 Jun.

Hans, D. (2000), "Computer-based patient record systems: network security issues", In: *http://www.saic.com/healthcare/downloads/computerbased.pdf*, acessado em 04 de outubro de 2005.

Huang, H.K. (2004), *PACS and Imaging Informatics – Basic Principles and Applications*, Hoboken:Wiley-Liss.

Huston, T.L. (2001), "Security issues for implementation of e-medical records", *Communications of the ACM*, v. 44, n. 9, p. 89-94.

Hutchinson, D., Warren, M. (2003), "Security for Internet banking: a framework", *Logistics Information Management*, v. 16, n. 1, p. 64-73.

Iachello, G., Abowd, G.D. (2005), "Privacy and proportionality: adapting legal evaluation techniques to inform design in ubiquitous computing", In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Portland, p. 91-100, 02-07 Apr.

IMIA (2004), "Código de Ética da IMIA para Profissionais de Informática em Saúde", In: http://www.sbis.org.br/codigo_etica_imia.htm, acessado em 10 de fevereiro de 2004.

IMIA (2005), "IMIA Working Groups – Security in Health Information Systems (Working Group 04)", In: http://www.imia.org/search.lasso?-database=organizations.fp5&-response=WG_profile.html&-layout=CGI&-sortField=workgroup_SIG&-sortOrder=ascending&-op=bw&type=WGSIG&-maxRecords=1&-skipRecords=15&-search, acessado em 10/12/2005.

Istepanian, R.S.H. (2005), "Wireless security for personalised and mobile healthcare services", In: *Proceedings 29th Annual International Computer Software and Applications Conference* [*COMPSAC 2005*], Edinburgh, v. 1, p. 86, 25-28 Jul.

JAHIS (2005), "JAHIS Standards", In: http://www.jahis.jp/standard/index.html, acessado em 13/12/2005.

Jaeger, T., Liedtke, J., Panteleenko, V., Park, Y., Islam, N. (1998), "Security architecture for component-based operating systems", In: *Proceedings of the 8th ACM SIGOPS European Workshop on Support for Composing Distributed Applications*, Sintra, p. 222-228, 7-10 Sep.

Jepsen, T. (2003), "IT in healthcare: progress report", *IEEE IT Professional*, v. 5, n. 1, p. 8-14.

Jøsang, A., Patton, M.A. (2003), "User interface requirements for authentication of communication", In: *4th Australasian User Interface Conference* [*AUIC2003*], Adelaide, p. 75-80, 04-07 Feb.

Jøsang, A., Sanderud, G. (2003), "Security in mobile communications: challenges and opportunities", In: *Proceedings of the Australasian Information Security Workshop Conference on ACSW Frontiers*, v. 21, p. 43-48.

Juramento de Hipócrates (2004), In: http://www.gineco.com.br/jura.htm, acessado em 07/05/2004.

Kara, A. (2001), "Protecting privacy in remote-patient monitoring", *IEEE Computer*, v. 34, n. 5, p. 24-27.

Kluge, E-H.W. (2004), "Informed consent and the security of the electronic health record (EHR): some policy considerations", *International Journal of Medical Informatics*, v. 73, n. 3, p. 229-234.

Knight, J.C. (2002), "Safety critical systems: challenges and directions", In: *Proceedings of the 24th International Conference on Software Engineering* [*ICSE'02*], Orlando, p. 547-550, 19-25 May.

Kobayashi, L.O.M, Furuie, S.S. (2004), "End-to-end security architecture for radiological images", In: *Proceedings of the 90th Scientific Assembly and Annual Meeting*, [*RSNA'2004*], Chicago, p. 172-172, 28 Nov-03 Dec.

Kobayashi, L.O.M, Furuie, S.S., Gutierrez, M.A. (2005), "Implementation of integrity and authenticity oriented to information flow for radiological images", In: *Proceedings of the 91st Scientific Assembly and Annual Meeting*, [*RSNA'2005*], Chicago, p. 397-397, 27 Nov-02 Dec.

Kobayashi, L.O.M., Motta, G.H.M.B., Furuie, S.S. (2004), "Análise dos requisitos tecnológicos para implementação de segurança fim-a-fim em imagens médicas", In: *Anais do XIX Brazilian Congress on Biomedical Engineering, III Congresso Latino Americano de Engenharia Biomédica* [*CLAEB'2004*], João Pessoa, p. 597-600, 22-25 Sep.

Kroll, M., Schütze, B., Geisbe, T., Lipinski, H.-G., Grönemeyer, D.H.W., Filler, T.J. (2003), "Embedded systems for signing medical images using the DICOM standard", *International Congress Series*, v. 1256, p. 849-854.

Kuo, C.H., Huang, F.G., Wang, K.L., Chen, H.W. (2003), "Design and implementation of Internet-based in-house healthcare and home automation systems", In: *IEEE International Conference on Systems, Man and Cybernetics*, Washington DC, v. 3, p. 2944-2949, Oct.

Kwak, Y.S. (2005), "International standards for building Electronic Health Record (EHR)", In: *Proceedings of 7th International Workshop on Enterprise networking and Computing in Healthcare Industry* [*HEALTHCOM 2005*], Busan, p. 18-23, 23-25 Jun.

Lederman, R. (2004), "The medical privacy rule: can hospitals comply using current health information systems?", In: *Proceedings of the 17th IEEE Symposium on Computer-Based Medical Systems* [*CBMS'04*], Bethesda, p. 236-241, 24-25 Jun.

Lee, K., Jiang, Z., Kim, S., Kim, S. (2005), "Security policy management for healthcare system network", In: *Proceedings of 7th International Workshop on Enterprise networking and Computing in Healthcare Industry* [*HEALTHCOM 2005*], Busan, p. 289-292, 23-25 Jun.

Lees, P.J., Chronaki, C.E., Simantirakis, E.N., Kostomanolakis, S.G., Orphanoudakis, S.C., Vardas, P.E. (1999), "Remote access to medical records via the Internet: feasibility, security and multilingual considerations", *Computers in Cardiology*, v. 26, p. 89-92.

Lettice, J. (2005), "NHS chief cans patient control over health record access", In: http://www.theregister.co.uk/2005/03/30/nhscrs_optout_canned/, acessado em 11 de abril de 2005.

Li, C.T., Lou, D.C., Chen, T.H. (2000), "Image authentication and integrity verification via content-based watermarks and a public key cryptosystem", In: *Proceedings of the IEEE International Conference on Image Processing*, Vancouver, v. 3, p. 694-697, 10-13 Sep.

Lin, L.S., Ramaiah, C.K., Wal, P.K. (2003), "Problems in the preservation of electronic records", *Library Review*, v. 52, n. 3, p. 117-125.

Liu, B.J., Zhou, Z., Huang, H.K. (2005), "A HIPAA-compliant architecture for securing clinical images", In: *Proceedings of SPIE Medical Imaging Conference*, San Diego, p. 326-333, 13-17 Feb.

Liu, T., Qiu, Z.D. (2002), "The survey of digital watermarking-based image authentication techniques", In: *Proceedings of the IEEE 6th International Conference on Signal Processing*, Beijin, v. 2, p. 1556-1559, 26-30 Aug.

Lorence, D.P., Churchill, R. (2005), "Incremental adoption of information security in health-care organizations: implications for document management", *IEEE Transactions on Information Technology in Biomedicine*, v. 9, n. 2, p. 169-173.

Lu, Y-C., Xiao, Y., Sears, A., Jacko, J.A. (2005), "A review and a framework of handheld computer adoption in healthcare", *International Journal of Medical Informatics*, v. 74, n. 5, p. 409-422.

Luz, A.R.A.V. (2004), *O prontuário eletrônico de paciente e a segurança da informação: uma abordagem arquivística*, Trabalho de Graduação, UniRio, Centro de Ciências Humanas.

Makris, L., Argiriou, N., Strintzis, M.G. (1997), "Network access and data security design for telemedicine applications", In: *Proceedings of Second IEEE Symposium on Computers and Communications*, Alexandria, p. 523-527, 01-03 Jul.

Malamateniou, F., Vassilacopoulos, G., Tsanakas, P. (1998), "A workflow-based approach to virtual patient record security", *IEEE Transactions on Information Technology in Biomedicine*, v. 2, n. 3, p. 139-145.

Marti, R., Delgado, J., Perramon, X. (2004), "Security specification and implementation for mobile e-health services", In: *2004 IEEE International Conference on e-Technology, e-Commerce and e-Service*, Taipei, p. 241-248, 28-31 Mar.

May, T.T. (1998), "Medical information security: the evolving challenge", In: *Proceedings of the 32nd Annual International Carnahan Conference on Security Technology*, p. 85-92, 12-14 Oct.

McFarland, M.C. (1991), "Standards-ethics and the safety of computer systems", *IEEE Computer*, v. 24, n. 2, p. 72-75.

MedSec (1997), "Health Care Security and Privacy in the Information Society", ISIS programme, EU, In: http://europa.eu.int/ISPO/isis/summary/projects/healthcare_networks/96medsec.htm.

Memon, N., Wong, P.W. (1998), "Protecting digital media

content", *Communications of the ACM*, v. 41, n. 7, p. 35-43.

Merger, O., Nitsche, U., Teufel, S. (1997), "Security concerns for mobile information systems in health care", In: *Proceedings of the 8th International Workshop on Database and Expert Systems Applications*, Toulouse, p. 312-317, 01-02 Sep.

Miaou, S-G., Hsu, C-M., Tsai, Y-S., Chao, H-M. (2000), "A secure data hiding technique with heterogeneous data-combining capability for electronic patient records", In: *Proceedings of the 22nd Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Chicago, v. 1, p. 280-283, 23-28 Jul.

Ministério Público Federal (2005), "Tabela de Temporalidade dos Documentos", 2005.

Mohan, J., Yaacob, R.R.R. (2004): "The Malaysian Telehealth Flagship Application: a national approach to health data protection and utilisation and consumer rights", *International Journal of Medical Informatics*, v. 73, n. 3, p. 217-227.

Moreira Filho, J.R. (2002), "Relação Médico-Paciente", In: http://www1.jus.com.br/doutrina/texto.asp?id=2745, acessado em 03 de junho de 2004.

Motta, G.H.M.B., Furuie, S.S. (2003), "A contextual role-based access control authorization model for electronic patient record", *IEEE Transactions on Information Technology in Biomedicine*, v. 7, n. 3, p. 202-207.

Mussi, C. (2005), *Certificação Eletrônica e Assinatura Digital Anvisa*, Apresentação, Anvisa.

Neame, R., Olson, M.J. (2004), "Security issues arising in establishing a regional health information infrastructure", *International Journal of Medical Informatics*, v. 73, n. 3, p. 285-290.

National Electrical Manufacturers Association – NEMA (2004), *Digital Imaging and Communications in Medicine (DICOM) Part 15: Security and System Management Profiles*, Rosslyn.

Neumann, P. G. (2005), "Risks to the Public", *ACM SIGSOFT Software Engineering Notes*, v. 30, n. 2, p. 17-25.

Niinimäki, J., Savolainen, M., Forsström J.J. (1998), "Methodology for security development of an electronic prescription system", In: *Proceedings of AMIA Symposium*, Orlando, p. 245-249, 07-11 Nov.

Nikolaidis, A., Tsekeridou, S., Tefas, A., Solachidis, V. (2001), "A survey on watermarking application scenarios and related attacks", In: *Proceedings of the IEEE International Conference on Image Processing*, Thessaloniki, v. 3, p. 991-994, 07-10 Oct.

Oates, J. (2005), "US hospital loses patient info", In: http://www.theregister.co.uk/2005/04/11/idtheft_hospital/, acessado em 11 de abril de 2005.

Olivier, M.S. (2002), "Database Privacy: balancing confidentiality, integrity and availability", *ACM SIGKDD Explorations Newsletter*, v. 4, n. 2, p. 20-27.

Organização das Nações Unidas (2004), "Declaração Universal dos Direitos Humanos, 1948", In: http://www.unhchr.ch/udhr/lang/por.htm, acessado em 07 de junho de 2004.

Owens, T.J., Tachakra, S., Banitsas, K.A., Istepanian, R.S.H. (2001), "Securing a Medical Wireless LAN System", In: *Proceedings of the 23rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Istanbul, v. 4, p. 3552-3555, 25-28 Oct.

Papadakis, I., Chrissikopoulos, V., Polemi, D. (2001), "Secure medical digital libraries", *International Journal of Medical Informatics*, v. 64, n. 2-3, p. 417-428.

Pereira, J., Lamelo, A., Vázquez-Naya, J.M., Fernández, M., López-Gestal, J.M., Teijero, J., Pazos, A. (2001), "Design and implementation of a DICOM PACS with secure access via Internet", In: *Proceedings of the 23rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Istanbul, v. 4, p. 3724-3727, 25-28 Oct.

Peterson, M.G.E. (2002), "Privacy versus safety: who is safe?", In: *Proceedings of the 15th IEEE Symposium on Computer-Based Medical Systems* [*CBMS'02*], Maribor, p. 85-90, 04-07 Jun.

Petruccio, A. (2000), "The Strategic Significance of Information Security", In: http://www.saic.com/healthcare/downloads/strategic.pdf, acessado pela última vez em 04 de outubro de 2005.

Pfitzmann, A., Pfitzmann, B. (1992), "Technical Aspects of Data Protection in Health Care Informatics", In: *Advances in Medical Informatics*, Eds.: J. Noothoven van Goor, J.P. Christensen, IOS Press, p. 368-386.

Power, D., Slaymaker, M., Politou, E., Simpson, A. (2005), "Protecting sensitive patient data via query modification", In: *Proceedings of the ACM Symposium on Applied Computing*, Santa Fe, p. 224-230, 13-17 Mar.

Raghupathi, W., Tan, J. (2002), "Strategic IT applications in health care", *Communications of the ACM*, v. 45 n. 12, p. 56-61.

Rector, A.L., Nowlan, W.A., Kay, S. (1991), "Foundations for an electronic medical record", *Methods of Information in Medicine*, v. 30, n. 3, p. 179-186.

Reni, G., Molteni, M., Arlotti, S., Pinciroli, F. (2004), "Chief medical officer actions on information security in an Italian rehabilitation centre", *International Journal of Medical Informatics*, v. 73, n. 3, p. 271-279.

Rindfleisch, T.C. (1997), "Privacy, information technology, and health care", *Communications of the ACM*, v. 40, n. 8, p. 92-100.

Roger-France, F.H. (2004), "Security of health care records in Belgium. Application in a University Hospital", *International Journal of Medical Informatics*, v. 73, n. 3, p. 235-238.

Ruotsalainen, P.A. (2004), "A cross-platform model for secure Electronic Health Record communication", *International Journal of Medical Informatics*, v. 73, n. 3, p. 291-295.

Ruotsalainen, P., Pohjonen, H. (2003), "European Security Frameworks for Health Care", In: *Advanced Health Telematics and Medicine: The Magdeburg Expert Summit Textbook*, Eds.: B. Blobel, P. Pharow, IOS Press.

SBIS – Sociedade Brasileira de Informática em Saúde (2004), "Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES), versão 2.1, 2004", In: http://www.sbis.org.br/manual.htm, acessado em 27 de fevereiro de 2004.

SBIS – Sociedade Brasileira de Informática em Saúde (2005), "SBIS - GT de Certificação de Software", In: http://www.sbis.org.br/certificacao.htm, acessado em 13/12/2005.

Schwaig, K.S., Kane, G.C., Storey, V.C. (2005), "Privacy, fair information practices and the fortune 500: the virtual reality of compliance", *The DATA BASE for Advances in Information Systems*, v. 36, n. 1, p. 49-63.

Shortliffe, E.H. (1998), "The evolution of health-care records in the era of the Internet", In: *Proceedings of the 9th World Congress on Medical Informatics* [*MedInfo98*], Seoul, p. 1-8, 18-22 Aug.

Shortliffe, E.H. (1999), "The evolution of electronic medical records", *Academic Medicine*, v. 74, n. 4, p. 414-419.

Smith, E., Eloff, J.H.P. (1999), "Security in health-care information systems – current trends", *International Journal of Medical Informatics*, v. 54, n. 1, p. 39-54.

Sohr, K., Drouineaud, M., Ahn, G-J. (2005), "Formal specification of role-based security policies for clinical information systems", In: *Proceedings of the ACM Symposium on Applied Computing*, Santa Fe, p. 332-339, 13-17 Mar.

Song, W.J., Ahn, B.H., Kim, W.H. (2002), "Healthcare information systems using digital signature and synchronized smart cards via the Internet", In: *Proceedings of the International Conference on Information Technology: Coding and Computing* [*ITCC'02*], Las Vegas, p. 177-182, 08-10 Apr.

Souza, N.T.C. (2002a), "Responsabilidade civil do médico", In: http://www1.jus.com.br/doutrina/texto.asp?id=2582, acessado em 03 de junho de 2004.

Souza, N.T.C. (2002b), "Responsabilidade civil do hospital", In: http://www1.jus.com.br/doutrina/texto.asp?id=2638, acessado em 03 de junho de 2004.

Stanford, V. (2002), "Pervasive health care applications face tough security Challenges", *IEEE Pervasive Computing*, v. 1, n. 2, p. 8-12.

Starida, K., Ganiatsas, G., Fotiadis, D.I., Likas, A. (2003), "CHILDCARE: a collaborative environment for the monitoring of children healthcare at home", In: *Proceedings of the4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine*, Birmingham, p. 169-172, 24-26 Apr.

Swire, P., Steinfeld, L. (2002), "Security and privacy after September 11: the health care example", In: *Proceedings of 12th Conference on Computers, Freedom & Privacy*, San Francisco, p. 1-13, 16-19 Apr.

Takeda, H., Matsumura, Y., Kuwata, S., Nakano, H., Sakamoto, N., Yamamoto, R. (2000), "Architecture for networked electronic patient record systems", *International Journal of Medical Informatics*, v. 60, n. 2, p. 161-167.

Takeda, H., Matsumura, Y., Kuwata, S., Nakano, H., Shanmai, J., Qiyan, Z., Yufen, C., Kusuoka, H., Matsuoka, M. (2004), "An assessment of PKI and networked electronic patient record system: lessons learned from real patient data exchange at the platform of OCHIS (Osaka Community Healthcare Information System)", *International Journal of Medical Informatics*, v. 73, n. 3, p. 311-316.

Ting, T.C. (1999), "Privacy and confidentiality in healthcare delivery information system", In: *Proceedings of the 12th IEEE Symposium on Computer-Based Medical Systems*, Stamford, p. 2-4, 18-20 Jun.

TISS (2006), "Segurança e Privacidade", In: http://www.ans.gov.br/portal/site/_hotsite_tiss/materia_20280.htm, acessado em 03 de fevereiro de 2006.

Toyoda, K. (1998), "Standardization and security for the EMR", *International Journal of Medical Informatics*, v. 48, n. 1-3, p. 57-60.

van der Haak, M., Wolff, A.C., Brandner, R., Drings, P., Wannenmacher, M., Wetter, T. (2003), "Data security and protection in cross-institutional electronic patient records", *International Journal of Medical Informatics*, v. 70, n. 2-3, p. 117-130.

Voas, J. (1999), "Protecting against what? The Achilles heel of information assurance", *IEEE Software*, v. 16, n. 1, p. 28-29.

Wang, C.X. (1999), "Security issues to tele-medicine system design", In: *IEEE Proceedings of the Southeastcon '99*, Lexington, p. 106-109, 25-28 Mar.

Waugh, A., Wilkinson, R., Hills, B., Dell'oro, J. (2000), "Preserving digital information forever", In: *Proceedings of the 5th ACM conference on Digital libraries*, San Antonio, p. 175-184, 02-07 Jun.

Weaver, A.C., Dwyer, S.J. III, Snyder, A.M., Van Dyke, J., Hu, J., Chen, X., Mulholland, T., Marshall, A. (2003), "Federated, secure trust networks for distributed healthcare IT services", In: *Proceedings of the 1st IEEE International Conference on Industrial Informatics* [*INDIN 2003*], Banff, p. 162-169, 21-24 Aug.

Wimalasiri, J.S., Ray, P., Wilson, C.S. (2004), "Maintaining security in an ontology driven multi-agent system for electronic health records", In: *Proceedings of the 6th International Workshop on Enterprise Networking and Computing in Healthcare Industry* [*HEALTHCOM 2004*], Odawara, p. 19-24, 28-29 Jun.

Wimalasiri, J.S., Ray, P., Wilson, C.S. (2005), "Security of electronic health records based on Web services", In: *Proceedings of 7th International Workshop on Enterprise networking and Computing in Healthcare Industry* [*HEALTHCOM 2005*], Busan, p. 91-95, 23-25 Jun.

Wohlmacher, P., Pharow, P. (2000), "Applications in health care using public-key certificates and attribute certificates", In: *16th Annual Conference on Computer Security Applications* [*ACSAC '00*], New Orleans, p. 128-137, 11-15 Dec.

Wong, P.W., (1998), "A public key watermark for image verification and authentication", In: *Proceedings of the 1998 International Conference on Image Processing* [*ICIP 98*], Chicago, v. 1, p. 455-459, 04-07 Oct.

Yee, G., Korba, L. (2005), "An agent architecture for e-services privacy policy compliance", In: *Proceedings of the 19th International Conference on Advanced Information Networking and Applications* [*AINA'05*], Taiwan, v.1, p. 374-379, 28-30 Mar.

Yee, G., Korba, L. (2004), "Privacy policy compliance for web services", In: *Proceedings of the IEEE International Conference on Web Services* [*ICWS'04*], San Diego, p. 158-165, 06-09 Jul.

Yu, P., Yu, H. (2004), "Lessons learned from the practice of mobile health application development", In: *Proceedings of the 28th Annual International Computer Software and Applications Conference* [*COMPSAC'04*], Hong Kong, v. 2, p. 58-59, 28-30 Sep.

Zain, J.M., Baldwin, L.P., Clarke, M. (2004), "Reversible watermarking for authentication of DICOM images", In: *Proceedings of the 26th Annual International Conference on Engineering in Medicine and Biology Society* [*EMBS 2004*], San Francisco, v. 2, p. 3237-3240, 01-04 Sep.

Zhang, L., Ahn, G.J., Chu, B.T. (2002), "A role-based delegation framework for healthcare information systems", In: *Proceedings of the7th ACM Symposium on Access Control*

*Models and Technologies* [*SACMAT' 02*], Monterey, p. 125-134, 03-04 Jun.

Zhou, X.Q., Huang, H.K., Lou, S.L. (2001), "Authenticity and integrity of digital mammography images", *IEEE Transactions on Medical Imaging*, v. 20, n. 8, p. 784-791.

Zhu, B., Swanson, M.D., Tewfik, A.H. (1996), "Transparent robust authentication and distortion measurement technique for images", In: *Proceedings of IEEE Digital Signal Processing Workshop*, Loen, p. 45-48, 01-04 Sep.